Aos meus pais

Agradecimentos

Ao meu orientador, Professor Doutor José Carlos Costa, pelo apoio e incentivo dado e pela disponibilidade e paciência, ao longo da elaboração desta dissertação.

Aos meus familiares e amigos, em especial à minha irmã e ao Miguel Barreto, que de uma forma ou de outra estiveram a meu lado e me deram todo o seu apoio.

Por último, não poderia deixar de agradecer à Escola Superior de Tecnologia e Gestão de Leiria, na pessoa do Professor Doutor Carlos Neves, por me terem dado as condições necessárias para a elaboração deste trabalho.

O problema da ω-palavra para pseudovariedades de semigrupos

Resumo

A teoria de semigrupos começou, de certa forma, com um resultado sobre semigrupos finitos: o Teorema de Suschekewitsch de 1928 descrevendo a estrutura dos semigrupos finitos sem ideais próprios. Nos anos 50, o desenvolvimento da teoria dos autómatos finitos trouxe motivação nova para o estudo de semigrupos finitos. No entanto, só desde os anos 70 é que esta teoria tem obtido cada vez mais atenção por parte dos investigadores sendo notório o seu crescimento.

Desde meados dos anos 60 surgiu a questão de como calcular a complexidade de um semigrupo finito S, questão esta, que quarenta anos volvidos continua a ser a principal motivação para muitos trabalhos sobre semigrupos finitos. O problema da decidibilidade para determinadas pseudovariedades é outro que continua a ocupar os investigadores.

Neste trabalho de síntese apresenta-se um pequeno estudo sobre o problema da ω-palavra para as pseudovariedades **Sl**, **N**, **K**, **D**, **LI**, **J** e **LSl**. É ainda referida uma solução para o problema da ω-palavra sobre **R**, o qual se provou recentemente ser decidível [13]. O problema da ω-palavra é o de decidir, para uma pseudovariedade e duas ω-palavras dadas, se a pseudovariedade verifica a igualdade das ω-palavras.

Um dos principais motivos de interesse deste estudo está relacionado com o facto de o problema da ω-palavra ser decidível para **V** poder aparecer como uma das condições necessárias para que a pseudovariedade **V** seja mansa. A noção de mansidão foi introduzida recentemente numa tentativa de definir propriedades mais fortes do que a decidibilidade que pudessem ser úteis para provar a decidibilidade de pseudovariedades definidas por operadores, tais como produto semidirecto, supremo, produto de Mal'cev, etc.

The ω-word problem for pseudovarieties of semigroups
Abstract

In a way, the semigroup theory started with a result about finite semigroup: the 1928 Suschekewitsch's theorem, describing the structure of finite semigroups without proper ideals. On the 50's, the development of the finite automata theory brought a new motivation for the study of finite semigroups. However, it's only since the 70's that this theory has obtained more and more attention from researchers experiencing a notable growth.

The question of how to calculate the complexity of a finite semigroup S has emerged in the midle 60's, question that even after forty years, is still the main motivation for many works about finite semigroups. The decidability problem for some pseudovarieties is another problem that still occupies researchers.

In this synthesis work is presented a small study about the ω-word problem in the pseudovarieties $\mathbf{Sl}$, $\mathbf{N}$, $\mathbf{K}$, $\mathbf{D}$, $\mathbf{LI}$, $\mathbf{J}$ e $\mathbf{LSl}$. It's also referred a solution of the ω-word problem over $\mathbf{R}$, which has been recently proved as being decidable [13]. The ω-word problem is the problem of deciding, for a pseudovariety and two given ω-terms, if the pseudovariety verifies the equality of the ω-terms.

One of the main interests of this study is related with the fact that the ω-word problem being decidable in $\mathbf{V}$ may appear as one of the necessary conditions for the pseudovariety $\mathbf{V}$ to be tame. The notion of tameness has recently emerged as a tentative of defining stronger properties others than decidability that could be useful to prove the decidability of pseudovarieties defined by operators, such as the semidirect product, join, Mal'cev product, etc.

Conteúdo

Introdução

A motivação principal para o estudo da teoria de semigrupos deve-se às suas aplicações em Informática, nomeadamente na teoria de autómatos e linguagens racionais.

Nos últimos 40 anos esta teoria teve um desenvolvimento considerável, o qual se fez sentir, em grande parte, a partir da publicação de um resultado de Krohn e Rhodes [28] e da publicação do tratado de Eilenberg [24]. Nesse tratado, Eilenberg introduziu o conceito de *pseudovariedade* de semigrupos, como sendo uma classe $\mathbf{V}$ de semigrupos finitos fechada para subsemigrupos, imagens homomorfas e produtos directos finitos. As pseudovariedades revelaram-se desde logo o meio mais adequado para estabelecer ligações com as teorias de linguagens racionais e autómatos passando assim a desempenhar um papel central na teoria.

No início dos anos 80, Reiterman [29] provou que as pseudovariedades são classes de semigrupos finitos definidas por *pseudoidentidades*, isto é, igualdades formais entre certos objectos designados *operações implícitas* (também chamadas *pseudo-palavras* ou *palavras profinitas*). Entre os exemplos mais usuais de operações implícitas encontram-se a multiplicação $a \cdot b$ e a ω-potência a^ω. O conceito de pseudo-palavra é uma generalização do de palavra sobre um alfabeto. Tem-se então que as palavras são um exemplo de pseudo-palavras. Refira-se ainda como exemplos usuais de operações implícitas as *ω-palavras*, que são exactamente aquelas que se podem construir a partir das letras usando, um número finito de vezes, a multiplicação e a ω-potência. Neste trabalho é apresentado o estudo do problema da ω-palavra para algumas pseudovariedades de semigrupos.

O trabalho está organizado do seguinte modo:

O primeiro capítulo é destinado a introduzir notações, definições e resultados básicos da teoria de semigrupos. As referências principais para a obtenção de mais pormenores e demonstrações são os livros de Howie [26], Almeida [4] e Eilenberg [24].

Como referência para o capítulo 2 pode ser usada a tese de doutoramento de J. C. Costa [21]. Dá-se início a este capítulo com a introdução dos conceitos de alfabeto e palavra. São também introduzidas notações e definições no que respeita às palavras finitas, infinitas e biinfinitas. Por último é apresentado um estudo sobre os factores das palavras biinfinitas que será útil para o quinto capítulo.

No terceiro capítulo, começa-se por definir variedades e pseudovariedades de semigrupos. Introduz-se o conceito de operação implícita e enuncia-se um teorema fundamental: o Teorema de Reiterman.

O quarto capítulo é todo ele dedicado ao problema da ω-palavra para as pseudovariedades $\mathbf{Sl}$, $\mathbf{N}$, $\mathbf{K}$, $\mathbf{D}$ e $\mathbf{LI}$.

No capítulo 5 apresenta-se a pseudovariedade $\mathbf{LSl}$. Mostra-se que podemos decidir efectivamente a igualdade entre duas ω-palavras de $\overline{\Omega}_A\mathbf{LSl}$.

No sexto capítulo, depois de estudadas as operações implícitas sobre a pseudovariedade $\mathbf{DS}$, mostra-se que sobre a pseudovariedade $\mathbf{J}$ todas as operações implícitas são ω-palavras e ainda que o problema da ω-palavra é decidível para essa pseudovariedade. Este capítulo é apresentado de uma forma muito próxima do que é feito no livro de J. Almeida [4].

No sétimo e último capítulo, após uma pequena abordagem de uma das linhas de investigação que tem vindo a ser seguida em torno do problema da decidibilidade de pseudovariedades, é apresentada uma solução para o problema da ω-palavra sobre $\mathbf{R}$, o qual se provou recentemente ser decidível [13].

Capítulo 1

Preliminares

1.1 Semigrupos

Diz-se que um par ordenado $(S, \cdot)$ é um *semigrupo* se S é um conjunto não vazio e $\cdot$ é uma operação binária associativa definida sobre S. Isto é, $\cdot$ é uma aplicação de $S \times S$ em S, que a cada elemento (x, y) de $S \times S$ associa um elemento $x \cdot y$ de S (o qual designaremos de *produto* de x por y), tal que, para quaisquer $x, y, z \in S$,

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

O número $|S|$ representa a cardinalidade do conjunto S e será designado a *ordem* de S. Se $|S|$ é finito, S diz-se um *semigrupo finito*, caso contrário, diremos que S é um *semigrupo infinito*.

Exemplos 1.1 *1) Os conjuntos $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ $(n \in \mathbb{N})$, munidos da relação adição ou multiplicação módulo n, são semigrupos finitos e $|\mathbb{Z}_n| = n$.*

2) Dada uma família não vazia $(S_i, \cdot_i)_{i\in I}$ de semigrupos, o seu produto directo $(\prod_{i\in I} S_i, \cdot)$ é um semigrupo cujo conjunto suporte é o produto cartesiano dos S_i $(i \in I)$ e o produto é definido por

$$(s_i)_{i\in I} \cdot (t_i)_{i\in I} = (s_i \cdot_i t_i)_{i\in I}.$$

Por convenção, $(\prod_{i\in\emptyset} S_i, \cdot)$ é o semigrupo trivial, ou seja, o semigrupo com um só elemento.

Quando daí não advier confusão, escreveremos habitualmente:

- S para designar um semigrupo $(S, \cdot)$;
- xy em vez de $x \cdot y$;
- x^n $(n \in \mathbb{N})$ em vez de $x \cdots x$, o produto de n elementos todos iguais a x.

Se S for um semigrupo tal que, para quaisquer $x, y \in S$,

$$xy = yx,$$

diremos que S é um semigrupo *comutativo*.

Um semigrupo $(M, \cdot)$ no qual existe $e \in M$ tal que, para todo o $x \in M$,

$$ex = xe = x,$$

diz-se um *monóide*. Note-se que para um monóide M qualquer, existe exactamente um elemento $e \in M$ com esta propriedade, o qual designaremos de *(elemento) identidade*. Geralmente, denotaremos esse elemento por 1 ou por 1_M.

A partir de um semigrupo S, é sempre possível construir um monóide, o qual designaremos de *monóide obtido de S por acréscimo de um elemento identidade se necessário* e denotaremos por S^1. Se S tem elemento identidade, então $S^1 = S$. Caso contrário $S^1 = S \cup \{1\}$, onde 1 é um elemento que não pertence a S e o produto em S^1 é uma extensão do produto em S de modo que 1 seja o elemento identidade, ou seja, para cada $s \in S$,

$$1s = s1 = s \quad \text{e} \quad 11 = 1.$$

Um semigrupo S que possui a seguinte propriedade

$$\forall a, b \in S\ \exists x, y \in S,\ ax = b \text{ e } ya = b,$$

diz-se um *grupo*. Esta não é a definição mais comum para grupo, mas é-lhe equivalente, na qual um grupo é definido como sendo um monóide G em que

$$\forall x \in G\ \exists x^{-1} \in G,\ x^{-1}x = xx^{-1} = 1_G.$$

Num grupo, os elementos x e x^{-1} são ditos *inversos* um do outro.

A um elemento z de um semigrupo S que verifique a condição

$$\forall x \in S,\ zx = z,$$

chama-se um *(elemento) zero à esquerda.* A noção de *(elemento) zero à direita* é definida dualmente. Se um semigrupo S possui um elemento que é simultaneamente zero à esquerda e zero à direita, então esse elemento é único e diz-se que é o *(elemento) zero* do semigrupo (habitualmente representado por 0 ou 0_S), e que S é um semigrupo com zero.

Exemplo 1.2 *Seja $S = [0, 1]$, o intervalo fechado dos reais entre zero e um e consideremos para cada $x, y \in S$, $x \cdot y = min(x, y)$. O par $(S, \cdot)$ é um semigrupo, no qual 0 é o elemento zero e 1 é o elemento identidade.*

Dado um semigrupo S, diz-se que S é um *semigrupo zero à esquerda* se verifica a condição

$$\forall x, y \in S, \ xy = x,$$

ou seja, se todos os elementos de S são zeros à esquerda. Dualmente, definimos um *semigrupo zero à direita.*

Um elemento e de um semigrupo S tal que $e = e^2$ diz-se um *idempotente.* Note-se que os elementos identidade e zero de um semigrupo, se existirem, são idempotentes. Denotaremos por

$$E(S) = \{e \in S \mid e^2 = e\}$$

o conjunto dos idempotentes de S.

Um semigrupo S diz-se um *semigrupo idempotente* ou uma *banda* se todos os seus elementos são idempotentes, ou seja, se $S = E(S)$. Uma banda comutativa diz-se um *semi-reticulado*. Tem-se como exemplo fundamental de um semi-reticulado o monóide $U_1 = \{0, 1\}$, com dois elementos, munido do produto $00 = 01 = 10 = 0$ e $11 = 1$. O semigrupo do Exemplo 1.2 constitui outro exemplo de um semi-reticulado.

Por uma *banda rectangular* entende-se um semigrupo, cujo conjunto suporte é da forma $A \times B$, com A e B conjuntos não vazios, e cuja multiplicação é dada, para todos os $a, a' \in A$ e $b, b' \in B$, por

$$(a, b)(a', b') = (a, b').$$

É imediato que estes semigrupos são bandas.

Um semigrupo S diz-se *nilpotente* se

$$\forall e \in E(S) \quad \forall s \in S, \quad es = se = e,$$

ou seja, se S possui um único idempotente e esse idempotente é o elemento zero.

Proposição 1.3 *Seja S um semigrupo finito. As condições seguintes são equivalentes:*

1. *S é nilpotente;*
2. *S possui elemento zero e existe $n \in \mathbb{N}$ tal que $S^n = 0$ (a notação S^n tem o significado usual e será formalmente introduzida na secção seguinte);*
3. *$\exists n \in \mathbb{N} \quad \forall x_1, \ldots, x_n, y_1, \ldots, y_n \in S, \quad x_1 \cdots x_n = y_1 \cdots y_n$.*

Um semigrupo S diz-se *localmente trivial* se

$$\forall e \in E(S) \quad \forall s \in S, \quad ese = e.$$

1.2 Subsemigrupos

Sendo A e B subconjuntos de um semigrupo S, denota-se

$$AB = \{ab \in S \mid a \in A, \ b \in B\}.$$

Para quaisquer $A, B, C \subseteq S$, tem-se $(AB)C = A(BC)$. Assim, o conjunto $\mathcal{P}(S)$ das partes de S munido desta multiplicação é um semigrupo, chamado o *semigrupo das partes* (ou *semigrupo potência*) de S.

Usaremos a notação A^n ($n \in \mathbb{N}$) em vez de $A \cdots A$, para representar o produto de n subconjuntos todos iguais a A. Para um elemento $b \in S$, escreveremos simplesmente Ab (resp. bA) em vez de $A\{b\}$ (resp. $\{b\}A$).

Sejam S um semigrupo e T um subconjunto não vazio de S. Diz-se que T é um *subsemigrupo* de S, e escreve-se $T \leq S$, se T é fechado para a operação em S, isto é,

$$\forall x, y \in T, \ xy \in T.$$

Dito de outra forma, T é um subsemigrupo de S se $T^2 \subseteq T$. Como a condição de associatividade se verifica para quaisquer elementos de S, em particular também se verifica para quaisquer elementos de T, donde se conclui que T é um semigrupo.

Exemplos 1.4 *Seja S um semigrupo. Então:*

1) S é um subsemigrupo de S.

2) Se S é um semigrupo com elemento zero e identidade, tem-se que $\{0\}$ e $\{1\}$ são seus subsemigrupos. Mais geralmente, sendo e qualquer elemento idempotente de S, $\{e\}$ é um subsemigrupo de S.

Um subsemigrupo T de S diz-se um *subgrupo* de S, denotando-se $T \leq_g S$, se T é um grupo. No caso de S ser um monóide, dizemos que T é um *submonóide* de S, escrevendo-se $T \leq_m S$, se T é um subsemigrupo de S que contém a identidade de S.

Exemplos 1.5 *Consideremos $S = [0, 1]$ o semigrupo do Exemplo 1.2. Então:*

1) O subconjunto $[0, \frac{1}{2}]$ é um subsemigrupo de S e é um monóide, mas não é um submonóide de S pois não contém o elemento identidade 1_S.

2) O subconjunto $\{\frac{1}{2}\}$ é um subgrupo de S.

Proposição 1.6 *Seja T um subconjunto não vazio de um semigrupo S. São equivalentes as afirmações seguintes:*

(i) *T é um subgrupo de S;*

(ii) $\forall x \in T,\ xT = Tx = T$.

1.3 Ideais

Dado um subconjunto não vazio I de um semigrupo S, diz-se que I é um *ideal* (resp. *ideal à esquerda*, *ideal à direita*) de S, se

$$S^1 I S^1 \subseteq I \quad (\text{resp. } S^1 I \subseteq I,\ IS^1 \subseteq I).$$

Note-se que I é um ideal de S, e escreve-se $I \trianglelefteq S$, se e somente se I é simultaneamente ideal à esquerda e ideal à direita de S.

Um ideal I de um semigrupo S é dito um ideal *minimal* de S se, para todo o ideal J de S,

$$J \subseteq I \Rightarrow J = I,$$

ou seja, se I é um ideal minimal para a relação de inclusão. Um ideal minimal, se existir, é único, e dizemos que é o *ideal mínimo* de S, também designado o *núcleo* de S. Note-se que nem todos os semigrupos têm ideal minimal.

A existência de ideal mínimo está assegurada em dois casos importantes.

Exemplos 1.7 *Seja S um semigrupo.*

1) Se S é finito, então S tem ideal mínimo (que se mostra ser o produto de todos os ideais de S).

2) Se S tem elemento zero, então $\{0\}$ é o ideal mínimo de S.

1.4 Homomorfismos

Uma aplicação $\varphi : S \to T$, onde S e T são semigrupos, diz-se um *homomorfismo* ou *morfismo* (de semigrupos) de S em T se

$$\forall x, y \in S,\ \varphi(xy) = \varphi(x)\varphi(y).$$

Para dois semigrupos S e T, dizemos ainda que:

- um homomorfismo φ de S em T é um *monomorfismo* se φ é uma aplicação injectiva;
- T é *imagem homomorfa* de S se existe um homomorfismo sobrejectivo (dito um *epimorfismo*) de S em T;
- S é *isomorfo* a T, e escreve-se $S \simeq T$, se existe um homomorfismo bijectivo (dito um *isomorfismo*) de S em T;
- T *divide* S, e escreve-se $T \prec S$, se T é imagem homomorfa de algum subsemigrupo de S.

Em geral, identificaremos dois semigrupos isomorfos.

1.5 Subsemigrupos gerados por uma parte do semigrupo

Se $\{T_i : i \in \mathbb{N}\}$ é uma família não vazia de subsemigrupos de um semigrupo S, então facilmente se verifica que a intersecção dos conjuntos $\{T_i : i \in \mathbb{N}\}$, ou é o conjunto vazio ou é um subsemigrupo de S.

Se X é um subconjunto não vazio de S, então a família dos subsemigrupos de S que contêm X é não vazia. De facto, o próprio S é um tal subsemigrupo, donde a intersecção da família é um subsemigrupo de S contendo X. Denota-se por $\langle X\rangle$ o *subsemigrupo de S gerado por X*, sendo caracterizado como o subsemigrupo de S que satisfaz as propriedades seguintes:

1) $X \subseteq \langle X\rangle$;

2) Se U é um subsemigrupo de S contendo X, então $\langle X\rangle \subseteq U$.

Ou seja, $\langle X\rangle$ é o menor subsemigrupo de S que contém X. Como se pode igualmente verificar $\langle X\rangle$ consiste de todos os elementos de S que podem ser escritos como produtos finitos de elementos de X, isto é, $x_1x_2\cdots x_n$, com $n \in \mathbb{N}$ e $x_1, x_2, \ldots, x_n \in X$.

De particular interesse é o caso em que o *conjunto de geradores* é um conjunto singular $X = \{x\}$, no qual escreveremos simplesmente $\langle x\rangle$ em vez de $\langle\{x\}\rangle$. Neste caso referimo-nos a

$$\langle x\rangle = \{x, x^2, x^3, \ldots\}$$

como o *subsemigrupo monogénico* gerado pelo elemento x. Se $\langle x\rangle$ é um conjunto finito com n elementos, diz-se que o elemento x tem *ordem (finita) n.* Caso contrário, diz-se que x tem *ordem infinita.* Se o semigrupo S satisfaz $S = \langle x\rangle$ para algum x pertencente a S, dizemos que S é *monogénico.*

O resultado seguinte é fundamental em teoria de semigrupos finitos.

Proposição 1.8 *Se S é um semigrupo finito e $x \in S$, então existe $k \in \mathbb{N}$ tal que x^k é um idempotente.*

Demonstração: Seja $x \in S$. Como S tem ordem finita, então também x tem ordem finita. Portanto, existem naturais distintos k e m tais que $x^k = x^m$.

Supondo $k < m$, seja $n = m - k$. Então $x^k = x^{k+n}$, donde

$$x^k = x^{k+n} = x^k x^n = x^{k+n} x^n = x^{k+2n},$$

e mais geralmente, para cada $q \in \mathbb{N}_0$,

$$x^k = x^{k+qn}.$$

Pelo algoritmo de Euclides, todo o natural $t \geq k$ pode ser escrito na forma $t = k + qn + r$ para alguns $q \in \mathbb{N}_0$ e $r \in \{0, 1, \ldots, n-1\}$. Logo,

$$x^t = x^{k+qn+r} = x^{k+qn} x^r = x^k x^r = x^{k+r}.$$

Conclui-se portanto que

$$\langle x \rangle = \{x, x^2, x^3, \ldots, x^{k+n-1}\}.$$

Considere-se, agora, o menor natural i tal que $x^i = x^j$, para algum $j > i$. Tome-se o menor natural p, tal que $x^i = x^{i+p}$. Então, pelo exposto anteriormente,

$$\langle x \rangle = \{x, x^2, \ldots, x^i, x^{i+1}, \ldots, x^{i+p-1}\},$$

e, pela escolha de i e p, os elementos $x, x^2, \ldots, x^{i+p-1}$ são todos distintos. Os números i e p são ditos, respectivamente, o *índice* e o *período* do elemento x.

Consideremos o subsemigrupo de $\langle x \rangle$, $G = \{x^i, x^{i+1}, \ldots, x^{i+p-1}\}$ e o grupo cíclico $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ dos inteiros módulo p. É um resultado básico de teoria de números que

$$\exists h \in \{0, \ldots, p-1\} \quad \overline{i+h} = \overline{1}.$$

Prova-se então que $\varphi : G \to \mathbb{Z}_p$, $x^{m(i+h)} \mapsto \overline{m}$ é um isomorfismo de semigrupos, e portanto tem-se que G é um grupo cíclico. Conclui-se assim que a identidade de G é o único idempotente de G e, consequentemente, o único idempotente de $\langle x \rangle$, pois por definição de i nenhum elemento da lista $x, x^2, \ldots, x^{i-1}$ é idempotente.$\Box$

Resulta da demonstração anterior que $\langle x \rangle$ contém um único idempotente. Tal idempotente é representado usualmente por x^ω.

Corolário 1.9 *Todo o semigrupo finito tem pelo menos um idempotente.*

Demonstração: Seja S um semigrupo finito e seja $x \in S$. Então x tem ordem finita e portanto, pela Proposição 1.8, $\langle x \rangle$ contém um idempotente. $\square$

Dado um semigrupo S, ao menor inteiro positivo n, caso exista, tal que para qualquer $x \in S$, x^n é um idempotente, chama-se o *expoente* de S.

O resultado seguinte afirma que existe sempre o expoente de um semigrupo finito.

Proposição 1.10 *Seja S um semigrupo finito. Então existe $n \in \mathbb{N}$ tal que para todo o $x \in S$, x^n é um idempotente.*

Demonstração: Consideremos $n = mmc\ \{r_x : x \in S\}$, onde r_x é o menor número natural tal que x^{r_x} é um idempotente. Uma vez que a Proposição 1.8 garante a existência de r_x, para todo o elemento x de S, conclui-se então que x^n é um idempotente, para qualquer $x \in S$. $\square$

Mostremos agora uma propriedade básica dos semigrupos finitos.

Proposição 1.11 *Sejam S um semigrupo finito e $|S|$ o seu cardinal. Então*

$$\forall n \geq |S|, \quad S^n = SE(S)S.$$

Demonstração: Seja $n \geq |S|$. A inclusão $SE(S)S \subseteq S^n$ é óbvia. Para provar a inclusão contrária seja $s = s_1 s_2 \cdots s_n \in S^n$ com $s_1, s_2, \ldots, s_n \in S$. Consideremos agora os seguintes elementos de S,

$$s_1,\ s_1 s_2,\ s_1 s_2 s_3, \ldots, s_1 s_2 \cdots s_n.$$

Como $n \geq |S|$, se estes produtos são todos distintos entre si, então o Corolário 1.9 garante que um deles, digamos $s_1 s_2 \cdots s_k$, é idempotente. Tem-se então

$$s = (s_1 s_2 \cdots s_k)(s_1 s_2 \cdots s_k)(s_{k+1} s_{k+2} \cdots s_n) \in SE(S)S.$$

Se os produtos em causa não são todos distintos, então existem $i, j \in \{1, \ldots, n\}$ com $i < j$, tais que

$$s_1 s_2 \cdots s_i = s_1 s_2 \cdots s_i s_{i+1} \cdots s_j.$$

Consequentemente, para todo o natural m,

$$s_1 s_2 \cdots s_i = s_1 s_2 \cdots s_i (s_{i+1} \cdots s_j)^m.$$

Como S é finito, pela Proposição 1.8, existe um natural r tal que $(s_{i+1}\cdots s_j)^r$ é idempotente. Assim,

$$s = s_1 s_2 \cdots s_i s_{i+1} \cdots s_j s_{j+1} \cdots s_n = s_1 s_2 \cdots s_i (s_{i+1} \cdots s_j)^r s_{j+1} \cdots s_n,$$

e deduz-se também neste caso que $s \in SE(S)S$. $\square$

1.6 Congruências

Uma relação de equivalência θ sobre um semigrupo S diz-se uma *congruência esquerda* de S, se

$$\forall a, b, x \in S,\ (a, b) \in \theta \Rightarrow (xa, xb) \in \theta.$$

A noção de *congruência direita* de S é definida dualmente. Uma relação de equivalência θ sobre um semigrupo S é uma *congruência* se θ é simultaneamente uma congruência esquerda e direita, o que é equivalente, como se pode provar, a ter-se

$$\forall a, b, c, d \in S,\ (a, b), (c, d) \in \theta \Rightarrow (ac, bd) \in \theta.$$

Sejam R uma relação de equivalência sobre um conjunto A e $a \in A$. A *classe de equivalência* de a definida pela relação R é o conjunto

$$[a]_R = \{b \in A \mid a\, R\, b\}.$$

Chama-se *conjunto quociente de A por R* ao conjunto de todas as classes de equivalência de R. Representa-se por A/R, e tem-se portanto

$$A/R = \{[a]_R \mid a \in A\}.$$

Se θ é uma congruência sobre um semigrupo S, o conjunto quociente S/θ munido da operação binária, definida para cada $a, b \in S$ por

$$[a]_\theta [b]_\theta = [ab]_\theta$$

é um semigrupo, chamado o *semigrupo quociente* de S por θ.

A aplicação

$$\begin{array}{rccc} \pi : & S & \rightarrow & S/\theta \\ & a & \mapsto & [a]_\theta \end{array}$$

é um epimorfismo, chamado o *epimorfismo canónico de S para S/θ*.

Exemplo 1.12 *Seja S um semigrupo. Para um ideal I de S, designa-se por* congruência de Rees sobre S de núcleo I *a relação de equivalência θ_I sobre S, definida por*

$$a\theta_I b \iff a = b \text{ ou } a, b \in I.$$

O semigrupo quociente S/θ_I denota-se usualmente por S/I.

Sejam ρ e σ relações binárias sobre um conjunto não vazio X. Notaremos por ρ^e a *equivalência* sobre X *gerada* por ρ, ou seja, ρ^e é a menor equivalência sobre X que contém ρ. A equivalência gerada por $\rho \cup \sigma$ será denotada por $\rho \vee \sigma$, ou seja,

$$\rho \vee \sigma = (\rho \cup \sigma)^e.$$

Quando as relações ρ e σ comutam, relativamente à composição, o cálculo de $\rho \vee \sigma$ fica bastante simplificado como o mostra a proposição seguinte.

Proposição 1.13 *Se ρ e σ são relações de equivalência sobre um conjunto X tais que $\rho \circ \sigma = \sigma \circ \rho$, então $\rho \vee \sigma = \rho \circ \sigma$.*

Recorde-se que,

$$\rho \circ \sigma = \{(a, b) \in X \times X \mid \exists c \in X \ : (a, c) \in \rho \ \wedge (c, b) \in \sigma\}.$$

1.7 Relações de Green

As relações de Green devem o seu nome a J. A. Green que as introduziu em 1951 e desempenham um papel fundamental no desenvolvimento da teoria de semigrupos. Algumas das mais importantes classes de semigrupos finitos podem ser definidas através delas.

Seja S um semigrupo. As relações de equivalência sobre S designadas por *relações de Green* são cinco: $\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{H}$ e $\mathcal{D}$. Comecemos por definir $\mathcal{R}, \mathcal{L}$ e $\mathcal{J}$. Estas relações de equivalência estão associadas às seguintes relações de *quasi--ordem* (isto é, reflexivas e transitivas): para $x, y \in S$,

$$\begin{aligned} x \leq_{\mathcal{R}} y &\Leftrightarrow xS^1 \subseteq yS^1 , \\ x \leq_{\mathcal{L}} y &\Leftrightarrow S^1x \subseteq S^1y , \\ x \leq_{\mathcal{J}} y &\Leftrightarrow S^1xS^1 \subseteq S^1yS^1 . \end{aligned}$$

Note-se que,

$$\begin{aligned} xS^1 \subseteq yS^1 &\Leftrightarrow x \in yS^1 \\ &\Leftrightarrow \exists u \in S^1, x = yu. \end{aligned}$$

Condições similares são válidas para as relações de quasi-ordem $\leq_{\mathcal{L}}$ e $\leq_{\mathcal{J}}$.

Assim, para $\mathcal{K} \in \{\mathcal{R}, \mathcal{L}, \mathcal{J}\}$, define-se para quaisquer $x, y \in S$

$$x\,\mathcal{K}\,y \quad \text{se e só se} \quad x \leq_{\mathcal{K}} y \quad \text{e} \quad y \leq_{\mathcal{K}} x.$$

Ou seja,

$$\begin{aligned} &x\,\mathcal{R}\,y \Leftrightarrow xS^1 = yS^1 \Leftrightarrow xu = y \text{ e } yv = x \text{ para alguns } u, v \in S^1, \\ &x\,\mathcal{L}\,y \Leftrightarrow S^1x = S^1y \Leftrightarrow ux = y \text{ e } vy = x \text{ para alguns } u, v \in S^1, \\ &x\,\mathcal{J}\,y \Leftrightarrow S^1xS^1 = S^1yS^1 \Leftrightarrow uxv = y \text{ e } ryt = x \text{ para alguns } u, v, r, t \in S^1. \end{aligned}$$

Resulta imediatamente da definição que $\mathcal{R} \subseteq \mathcal{J}$ e $\mathcal{L} \subseteq \mathcal{J}$. Sendo também evidente que

$$xu \leq_{\mathcal{R}} x, \quad ux \leq_{\mathcal{L}} x \quad \text{e} \quad uxv \leq_{\mathcal{J}} x$$

para qualquer $x \in S$ e quaisquer $u, v \in S^1$.

As duas restantes relações de Green ($\mathcal{H}$ e $\mathcal{D}$), são definidas através das relações $\mathcal{R}$ e $\mathcal{L}$:

$$\mathcal{H} = \mathcal{R} \cap \mathcal{L} \quad \text{e} \quad \mathcal{D} = \mathcal{R} \vee \mathcal{L}.$$

Como se pode verificar, as compostas $\mathcal{R} \circ \mathcal{L}$ e $\mathcal{L} \circ \mathcal{R}$ coincidem em cada semigrupo e portanto, pela Proposição 1.13, obtém-se a caracterização mais simples e útil

$$\mathcal{D} = \mathcal{R} \vee \mathcal{L} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}.$$

Define-se ainda a relação de quasi-ordem $\leq_{\mathcal{H}}$ sobre S da seguinte forma

$$x \leq_{\mathcal{H}} y \quad \Leftrightarrow \quad x \leq_{\mathcal{R}} y \quad \text{e} \quad x \leq_{\mathcal{L}} y.$$

O resultado que se segue é de grande importância no estudo dos semigrupos finitos.

Proposição 1.14 *Se S é um semigrupo finito, então $\mathcal{D} = \mathcal{J}$.*

Seja S um semigrupo. Para qualquer das relações de Green $\mathcal{K}$ sobre S, denotaremos por K_x a $\mathcal{K}$-classe contendo um dado elemento $x \in S$. Diz-se que S é $\mathcal{K}$-*trivial* se $\mathcal{K}$ é a relação de igualdade em S, isto é, se $K_x = \{x\}$ para todo o elemento $x \in S$. Se $\mathcal{K}$ é a relação universal em S, ou seja, se $K_x = S$ para todo o elemento $x \in S$, então S diz-se $\mathcal{K}$-*universal*.

Exemplo 1.15 *Seja A um conjunto finito. O semigrupo $(\mathcal{P}(A), \cap)$ é $\mathcal{J}$-trivial. De facto, dados $X, Y \in \mathcal{P}(A)$ tais que $X \mathcal{J} Y$, deduz-se*

$$\begin{aligned} X \mathcal{J} Y &\Rightarrow B \cap X \cap C = Y \text{ e } D \cap Y \cap E = X, \text{ para alguns } B, C, D, E \in \mathcal{P}(A) \\ &\Rightarrow Y \subseteq X \text{ e } X \subseteq Y \\ &\Rightarrow Y = X. \end{aligned}$$

1.8 A estrutura das $\mathcal{D}$-classes

Cada $\mathcal{D}$-classe num semigrupo S é tanto uma união de $\mathcal{R}$-classes como de $\mathcal{L}$--classes, enquanto a intersecção não vazia de uma $\mathcal{R}$-classe e de uma $\mathcal{L}$-classe é uma $\mathcal{H}$-classe. Esta observação sugere a representação das $\mathcal{D}$-classes como "caixas de ovos", segundo a qual os elementos de cada $\mathcal{D}$-classe são organizados num rectângulo de quadrados onde cada quadrado constitui uma $\mathcal{H}$-classe, cada

$$\begin{array}{r c} & \begin{array}{cccc} \mathcal{L}\text{-classe} & & & \mathcal{L}\text{-classe} \\ \downarrow & & & \downarrow \end{array} \\ \begin{array}{r} \mathcal{R}\text{-classe} \rightarrow \\ \\ \\ \mathcal{R}\text{-classe} \rightarrow \end{array} & \begin{array}{|c|c|c|c|} \hline \quad & \quad & \cdots & \quad \\ \hline & & \cdots & \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline & & \cdots & \\ \hline \end{array} \end{array}$$

linha de quadrados uma $\mathcal{R}$-classe e cada coluna de quadrados uma $\mathcal{L}$-classe. Para indicar que uma dada $\mathcal{H}$-classe contém um idempotente é frequente representar um asterisco no quadrado correspondente a essa $\mathcal{H}$-classe.

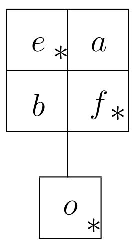
Exemplo 1.16 *Consideremos o semigrupo* $B_2 = \{o, e, f, a, b\}$ *de matrizes, onde os elementos* o, e, f, a, b *são, respectivamente, as matrizes*

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

A tabela de Cayley de B_2 *é dada por*

$\cdot$	o	e	f	a	b
o	o	o	o	o	o
e	o	e	o	a	o
f	o	o	f	o	b
a	o	o	a	o	e
b	o	b	o	f	o

O semigrupo B_2 *pode ser representado pelo seguinte diagrama, que descreve a organização dos seus elementos de acordo com as relações de Green.*



Como se verifica pelo diagrama, este semigrupo tem duas $\mathcal{D}$*-classes, sendo elas* $\{o\}$ *e* $\{e, b, f, a\}$*. Possui três* $\mathcal{L}$*-classes, três* $\mathcal{R}$*-classes e cinco* $\mathcal{H}$*-classes, sendo* $\mathcal{H}$*-trivial.*

Lema 1.17 (Lema de Green) *Sejam* a, b *elementos* $\mathcal{R}$*-equivalentes de um semigrupo* S *e sejam* $s, t \in S^1$ *tais que*

$$as = b \quad e \quad bt = a.$$

Então as correspondências

$$\begin{array}{rrcl} \rho_s: & L_a & \rightarrow & L_b \\ & x & \mapsto & xs \end{array} \qquad e \qquad \begin{array}{rrcl} \rho_t: & L_b & \rightarrow & L_a \\ & x & \mapsto & xt \end{array}$$

são aplicações bijectivas mutuamente inversas que preservam as $\mathcal{H}$*-classes.*

Demonstração: Mostremos primeiro, que ρ_s está bem definida. Seja $x \in L_a$. Então, tem-se

$$\begin{aligned} x \in L_a &\Rightarrow x \mathcal{L} a \Rightarrow S^1x = S^1a \Rightarrow S^1xs = S^1as \Rightarrow xs \mathcal{L} as \\ &\Rightarrow \rho_s(x) \in L_b. \end{aligned}$$

Conclui-se assim, que ρ_s é de facto uma aplicação de L_a em L_b.

Como por hipótese $x \in L_a$, então existe $u \in S^1$ tal que $x = ua$, donde

$$\rho_t \circ \rho_s(x) = \rho_t(xs) = xst = uast = ubt = ua = x,$$

o que mostra que $\rho_t \circ \rho_s$ é a aplicação identidade sobre L_a. Aplicando os mesmos argumentos mostra-se que ρ_t é uma aplicação de L_b em L_a e que $\rho_s \circ \rho_t$ é a aplicação identidade sobre L_b. Assim conclui-se a primeira parte do resultado.

Para provar a última parte do resultado, consideremos $x, y \in L_a$, e suponhamos que $x \,\mathcal{H}\, y$. Então $x \,\mathcal{R}\, y$ e $x \,\mathcal{L}\, y$. Da segunda condição resulta imediatamente que $xs \,\mathcal{L}\, ys$, ou seja, $\rho_s(x) \,\mathcal{L}\, \rho_s(y)$. Por outro lado, como ρ_s e ρ_t são bijecções mutuamente inversas deduz-se $x = xst$ e $y = yst$, portanto $x \mathcal{R} xs$ e $y \mathcal{R} ys$. Agora, como $x \mathcal{R} y$ pode concluir-se que $xs \mathcal{R} ys$, ou seja, $\rho_s(x) \mathcal{R} \rho_s(y)$. Portanto $\rho_s(x) \mathcal{H} \rho_s(y)$. Reciprocamente, admitindo que $xs \mathcal{H} ys$, deduz-se $xst \mathcal{H} yst$, ou seja $x \mathcal{H} y$. Mostramos assim que $x \mathcal{H} y$ se e só se $\rho_s(x) \mathcal{H} \rho_s(y)$, i.e., ρ_s preserva as $\mathcal{H}$-classes. De modo análogo mostra-se que ρ_t preserva as $\mathcal{H}$-classes. □

O Lema de Green admite o seguinte resultado análogo para as $\mathcal{R}$-classes.

Lema 1.18 (Lema de Green (dual)) *Sejam a, b elementos $\mathcal{L}$-equivalentes de um semigrupo S e sejam $s, t \in S^1$ tais que*

$$sa = b \quad e \quad tb = a.$$

Então as correspondências

$$\begin{array}{rccc} \lambda_s : & R_a & \rightarrow & R_b \\ & x & \mapsto & sx \end{array} \qquad e \qquad \begin{array}{rccc} \lambda_t : & R_b & \rightarrow & R_a \\ & x & \mapsto & tx \end{array}$$

são aplicações bijectivas mutuamente inversas que preservam as $\mathcal{H}$-classes.

Como consequência do Lema de Green e do seu dual deduz-se o seguinte resultado.

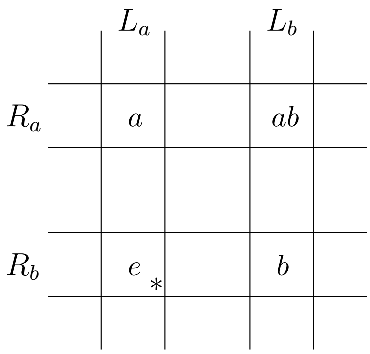
Corolário 1.19 *Seja S um semigrupo e sejam a, b elementos de S. Se $a \,\mathcal{D}\, b$, então $|H_a| = |H_b|$.*

Demonstração: Como por hipótese $a \,\mathcal{D}\, b$, então existe $c \in S^1$ tal que $a \,\mathcal{R}\, c$ e $c \mathcal{L}\, b$, donde

$$cr = a, \quad as = c, \quad tc = b, \quad ub = c,$$

para alguns $r, s, t, u \in S^1$. Pelos Lemas 1.17 e 1.18 deduz-se que $\rho_s|_{H_a}$ é uma bijecção de H_a para H_c e $\lambda_t|_{H_c}$ é uma bijecção de H_c para H_b. Portanto $\lambda_t \circ \rho_s|_{H_a}$ é uma bijecção de H_a para H_b (com inversa $\rho_r \circ \lambda_u|_{H_b}$), e daí resulta que $|H_a| = |H_b|$. □

Proposição 1.20 *Para quaisquer dois elementos $a, b \in S$, $ab \in R_a \cap L_b$ se e só se $R_b \cap L_a$ contém um idempotente.*



Demonstração: Suponhamos que $ab \in R_a \cap L_b$. Então $ab \,\mathcal{R}\, a$ e $L_{ab} = L_b$, e assim, pelo Lema de Green, $\rho_b : L_a \to L_b$, $x \mapsto xb$, é uma bijecção que preserva as $\mathcal{H}$-classes. Logo, existe $e \in L_a \cap R_b$ tal que $\rho_b(e) = b$, ou seja, $eb = b$. Dado que $e \mathcal{R} b$, existe $t \in S^1$ tal que $e = bt$. Segue-se, $(bt)b = eb = b$, e consequentemente, $e^2 = (bt)(bt) = (btb)t = bt = e$, ou seja, e é um idempotente.

Reciprocamente, se $e = e^2 \in R_b \cap L_a$, então $e \,\mathcal{R}\, b$ e $e \,\mathcal{L}\, a$, donde $er = b$ e $se = a$ para alguns $r, s \in S^1$. Logo,

$$eb = e(er) = (ee)r = er = b \quad \text{e} \quad ae = (se)e = s(ee) = se = a.$$

Como $e \mathcal{R} b$ e $e \mathcal{L} a$, deduz-se que $ae \mathcal{R} ab$ e $eb \mathcal{L} ab$. Ou seja, $a \mathcal{R} ab$ e $b \mathcal{L} ab$, o que prova que $ab \in R_a \cap L_b$. □

Dos resultados anteriores deduz-se os seguintes corolários importantes.

Corolário 1.21 *Seja H uma $\mathcal{H}$-classe de um semigrupo S. As condições seguintes são equivalentes:*

i) *H contém um idempotente;*

ii) *$H^2 \cap H \neq \emptyset$ (i.e., existem $a, b \in H$ tais que $ab \in H$);*

iii) *$H^2 = H$ e, neste caso, H é um subgrupo de S.*

Corolário 1.22 *Se e é um idempotente de um semigrupo S, então H_e é um subgrupo de S. Nenhuma $\mathcal{H}$-classe de S pode conter mais do que um idempotente.*

Outro resultado importante é o seguinte, cuja demonstração pode ser encontrada em [27].

Proposição 1.23 *Seja S um semigrupo finito. Se $a, b \in S$ são tais que $a \leq_{\mathcal{J}} b$, então:*

1. *se $b \leq_{\mathcal{R}} a$ então $a \mathcal{R} b$;*
2. *se $b \leq_{\mathcal{L}} a$ então $a \mathcal{L} b$;*
3. *se $b \leq_{\mathcal{H}} a$ então $a \mathcal{H} b$.*

Refira-se ainda que todo o semigrupo finito S possui uma $\mathcal{J}$-classe mínima (em relação à ordem parcial definida sobre as $\mathcal{J}$-classes). Prova-se que esta $\mathcal{J}$-classe mínima, J, é o ideal mínimo de S. Com base no Corolário 1.21, podemos verificar que J é constituída por $\mathcal{H}$-classes que são grupos. Suponhamos então que H é uma $\mathcal{H}$-classe e que H está contida em J. Se $H^2 = H$, então H é grupo. Caso contrário, existem $a, b \in H$ tais que $ab \notin H$, e prova-se que $J_{ab} < J_a$ o que é absurdo porque J é mínima.

1.9 Elementos regulares de um semigrupo

Um elemento a de um semigrupo S diz-se *regular* se existe $x \in S$ tal que $axa = a$. O elemento x é chamado um *associado* de a. O conjunto dos associados de a é representado por $A(a)$. Se todos os elementos de S são regulares, dizemos que S é um *semigrupo regular*.

Sejam S um semigrupo e $a \in S$. Dizemos que $a' \in S$ é um *inverso* de a se

$$aa'a = a \quad \text{e} \quad a'aa' = a'.$$

Ou seja, a' é um inverso de a se $a' \in A(a)$ e $a \in A(a')$. O conjunto dos inversos de a é representado por $V(a)$. Note-se que um elemento de S que admite um inverso é necessariamente regular. De igual modo, todo o elemento regular $a \in S$ tem um inverso: se $x \in A(a)$, então $xax \in V(a)$. Um elemento pode ter mais do que um inverso.

Exemplos 1.24 *Seja S um semigrupo e seja $a \in S$.*

1) Se S é um grupo, então S é um semigrupo regular e $A(a) = \{a^{-1}\}$;

2) Se S é uma banda rectangular, então S é um semigrupo regular. Tem-se $A(a) = S$ e $V(a) = S$ para cada $a \in S$;

3) Todo o elemento $e \in E(S)$ é regular ($eee = e$).

Passemos agora a demonstrar uma proposição que dá diversas caracterizações das $\mathcal{D}$-classes regulares de um semigrupo.

Proposição 1.25 *Seja D uma $\mathcal{D}$-classe de um semigrupo finito S. Então, as seguintes condições são equivalentes:*

i) D é regular;

ii) D contém algum elemento regular;

iii) cada $\mathcal{R}$-classe de D contém algum idempotente;

iv) cada $\mathcal{L}$-classe de D contém algum idempotente;

v) D contém algum idempotente;

vi) existem $a, b \in D$ tais que $ab \in D$.

Demonstração: Prova-se, inicialmente, que a é regular se e só se R_a contém algum idempotente.

Suponhamos que a é regular. Então $axa = a$, para algum $x \in S$. Agora, tomando $e = ax$, verifica-se que $a \,\mathcal{R}\, e$. Note-se que e é idempotente, pois, $e = ax = (axa)x = (ax)(ax) = e^2$.

Reciprocamente, se $a \mathcal{R} e$, para algum idempotente e, então existem $x, y \in S^1$ tais que $ax = e$ e $ey = a$. Assim, deduz-se que $ea = e(ey) = e^2y = ey = a$ e, portanto, que $a = ea = e^2a = axea$, ou seja, que a é regular. Analogamente, prova-se que a é regular se e só se L_a contém algum idempotente.

Sejam $a, b \in D$ tais que a é regular. Dado que $a \,\mathcal{D}\, b$, existe $c \in S$ tal que $a \mathcal{R} c$ e $c \,\mathcal{L}\, b$. Como por hipótese a é regular, $R_a = R_c$ contém um idempotente e por isso c é regular. Portanto, $L_c = L_b$ contém um idempotente e consequentemente b é regular. Isto estabelece a equivalência das quatro primeiras condições. Por outro lado, que *iii*) implica *v*) é evidente. Que *v*) implica *ii*) também é evidente (pois, já foi referido que todo o elemento idempotente é regular). Finalmente a equivalência entre *v*) e *vi*) resulta da Proposição 1.23 e da Proposição 1.20. □

Note-se que, pela Proposição 1.25 (cujas cinco primeiras condições são equivalentes para semigrupos quaisquer), é imediato que para D, uma $\mathcal{D}$-classe de um semigrupo S, ou todos os elementos de D são regulares ou nenhum elemento de D é regular. Se todos os elementos são regulares D diz-se uma *$\mathcal{D}$-classe regular*, caso contrário diz-se uma *$\mathcal{D}$-classe irregular*.

Para finalizar apresentamos certas classes de semigrupos que podem ser definidas através das relações de Green, como havíamos referido anteriomente, ou por condições de regularidade. Por exemplo, prova-se que um semigrupo S é um grupo se e só se $\mathcal{H}$ é a relação universal sobre S.

Definição 1.26 *Um semigrupo S diz-se:*

1. *aperiódico, se $\mathcal{H}$ é a relação trivial sobre S;*
2. *simples, se $\mathcal{J}$ é a relação universal sobre S;*
3. *inverso, se é regular e cada elemento tem um e um só inverso;*
4. *ortodoxo, se é regular e os seus idempotentes formam um subsemigrupo.*

Como exemplos de semigrupos simples temos as bandas rectangulares. Os grupos e os semi-reticulados constituem exemplos de semigrupos inversos.

Capítulo 2

Palavras

2.1 Palavras finitas

Chama-se *alfabeto* a um conjunto A finito não vazio. Os elementos de A são chamados *letras*. Uma sequência finita $a_1a_2\cdots a_n$ de letras de A diz-se uma *palavra* sobre A. A sequência vazia denota-se por 1 e diz-se a *palavra vazia*.

Representa-se por A^* o conjunto de todas as palavras sobre A e A^+ denota o conjunto $A^* \setminus \{1\}$. Munindo o conjunto A^+ (resp. A^*) com a operação binária $\cdot$ definida, para quaisquer duas palavras $u = a_1 \cdots a_n$ e $v = b_1 \cdots b_m$ de A^+, por

$$u \cdot v = a_1a_2 \cdots a_n \cdot b_1b_2 \cdots b_m = a_1a_2 \cdots a_nb_1b_2 \cdots b_m = uv,$$

$$(u \cdot 1 = a_1a_2 \cdots a_n \cdot 1 = a_1a_2 \cdots a_n = u = 1 \cdot u \text{ e } 1 \cdot 1 = 1)$$

chamada o *produto (de concatenação)* de palavras, obtém-se um semigrupo (resp. monóide), designado o *semigrupo livre gerado por A* (resp. *monóide livre gerado por A*). A justificação desta designação encontra-se na propriedade do próximo resultado. Ou seja, A^+ é *livre* sobre A no seguinte sentido.

Proposição 2.1 *Seja S um semigrupo. Se $\varphi : A \to S$ é uma aplicação qualquer, existe um e um só morfismo $\overline{\varphi} : A^+ \to S$ tal que o diagrama*

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & S \\ & A^+ \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

comuta (ou seja, $\varphi = \overline{\varphi} \circ \iota$*), onde* ι *é a aplicação de inclusão de* A *sobre* A^+*.*

Demonstração: O morfismo $\overline{\varphi}$ é definido, para cada $u = a_1 a_2 \cdots a_n \in A^+$, em que $a_i \in A$ para todo o i, por

$$\overline{\varphi}(u) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n),$$

e diz-se o *prolongamento natural* de φ a A^+. □

Note-se que A^* não é um monóide comutativo em geral. Considerando por exemplo, $A = \{a, b, c\}$, $u = aba$ e $v = ac$ obtém-se $uv = abaac \neq acaba = vu$. No entanto, as leis do corte são válidas no monóide A^*, i.e., dadas palavras $u, v, w \in A^*$,

$$uv = uw \;\Rightarrow\; v = w \quad \text{(lei do corte à esquerda)}$$
$$vu = wu \;\Rightarrow\; v = w \quad \text{(lei do corte à direita).}$$

Dada uma palavra u sobre um alfabeto A, denota-se por $|u|$, o *comprimento* da palavra u, que é o número de ocorrências de letras de A em u. O comprimento da palavra vazia é zero. Para $a \in A$, representa-se por $|u|_a$ o número de ocorrências da letra a em u. Por exemplo, sendo $A = \{a, b, c\}$, tem-se $|b| = 1$, $|acaba| = 5$, $|acaba|_a = 3$, $|acaba|_b = 1$ e $|b|_c = 0$. Note-se que, para um alfabeto A qualquer, $u, v \in A^*$ e $a \in A$ tem-se

$$|uv| = |u| + |v|, \quad |uv|_a = |u|_a + |v|_a, \quad |u| = \sum_{a \in A} |u|_a.$$

O *conteúdo* de uma palavra $u \in A^*$ é o conjunto de todas as letras de A que ocorrem em u e denota-se por $c(u)$.

Sejam u e w duas palavras de A^*. Diz-se que

- u é um *factor* de w se existem $x, y \in A^*$ tais que $w = xuy$;
- u é um *prefixo* (resp. *sufixo*) de w se existe $y \in A^*$ tal que $w = uy$ (resp. $w = yu$);
- um *factor* (resp. *sufixo*, *prefixo*) u de w é *próprio* se $u \neq w$.

Seja $k \in \mathbb{N}_0$. Para cada palavra $u \in A^*$ de comprimento maior ou igual a k, denota-se por $p_k(u)$ (resp. $s_k(u)$) o prefixo (resp. sufixo) de u de comprimento k.

Exemplo 2.2 *Para* $A = \{a, b, c\}$ *e* $u = abca$ *os factores de* u *são* 1, a, b, c, ab, bc, ca, abc, bca *e* u*; os prefixos de* u *são* $p_0(u) = 1$, $p_1(u) = a$, $p_2(u) = ab$, $p_3(u) = abc$ *e* $p_4(u) = u$. *Note-se que todos os prefixos de comprimento menor ou igual a três são próprios. Finalmente,* 1, a, ca, bca *e* u *são sufixos de* u.

Consideremos $u, v \in A^+$. Para indicar o número de ocorrências do factor v em u escreve-se $\begin{bmatrix} u \\ v \end{bmatrix}$. Por exemplo $\begin{bmatrix} bbababaa \\ bab \end{bmatrix} = 2$, pois bab ocorre duas vezes na palavra $bbababaa$: $b\,\underline{bab}\,abaa$, $bba\,\underline{bab}\,aa$.

Diz-se que uma palavra $u \in A^+$ é *primitiva* se

$$u = v^n, \text{ com } v \in A^+ \text{ e } n \in \mathbb{N} \;\Rightarrow u = v \text{ (e } n = 1),$$

ou seja, u não é potência de uma outra palavra.

Duas palavras $u, v \in A^+$ dizem-se *conjugadas* se existem $x, y \in A^*$ tais que

$$u = xy, \quad v = yx.$$

Lema 2.3 *Sejam* $u, v \in A^+$. *Se* u *é primitiva e* v *é conjugada de* u*, então* v *também é primitiva.*

Demonstração: Por hipótese v é conjugada de u, e portanto,

$$\exists w, z \in A^* : \quad u = wz \quad \text{e} \quad v = zw.$$

Suponhamos que $v = r^k$, onde $r \in A^+$ e $k \in \mathbb{N}$. Então, existem $x, y \in A^*$ e $k_1, k_2 \in \mathbb{N}_0$ tais que $r = xy,\ z = r^{k_1}x,\ w = yr^{k_2}$ e $k_1 + k_2 + 1 = k$. Portanto,

$$u = wz = yr^{k_2}r^{k_1}x = (yx)^k,$$

e como u é primitiva, $k = 1$. Logo, $v = r$. Conclui-se assim que v é primitiva. $\Box$

Proposição 2.4 ([31]) *Sejam* $u, v \in A^*$. *Se existem duas potências* u^k *e* v^n *de* u *e de* v*, respectivamente, com o mesmo prefixo (ou sufixo) de comprimento pelo menos igual a* $|u| + |v| - mdc(|u|, |v|)$*, então* u *e* v *são potências de uma mesma palavra.*

Corolário 2.5 *Sejam* $u, v \in A^+$ *e seja* $a \in A$ *tal que* $s_1(u) \neq a$ *(resp.* $p_1(u) \neq a$*). Para* $k \in \mathbb{N}$ *tal que* $|u^k| \geq |u| + |v| - mdc(|u|, |v|)$*, então* au^k *(resp.* u^ka*) não é factor de* v^p*, qualquer que seja* $p \in \mathbb{N}$.

Demonstração: Consideremos $|u| + |v| - mdc(|u|, |v|) = n$. Suponhamos que o corolário é falso, ou seja, que au^k é factor de algum v^p. Então,

$$au^k = (aw_1)^m w_2,$$

com aw_1 conjugado de v, $w_2 \in A^*$ prefixo próprio de aw_1 e $m \geq 1$.

- Se $w_2 \neq 1$, então

  $$au^k = (aw_1)^m w_2 = (aw_1)(aw_1)\dots(aw_1)w_2 = a(w_1a)\dots(w_1a)(w_1a)w_3,$$

  onde $aw_3 = w_2$.

  Portanto tem-se $u^k = (w_1a)^t w_3$, onde $t = m$.

- Se $w_2 = 1$, então

  $$au^k = (aw_1)^m w_2 = (aw_1)^m = (aw_1)(aw_1)\dots(aw_1) = a(w_1a)\dots(w_1a)w_1.$$

  Assim $u^k = (w_1a)^t w_3$, onde $w_3 = w_1$ e $t = m - 1$.

Conclui-se assim que $u^k = (w_1a)^t w_3$ para alguns $t \in \mathbb{N}_0$ e $w_3 \in A^*$. Então, u e w_1a admitem potências com o mesmo prefixo de comprimento pelo menos igual a n. Portanto, pela Proposição 2.4, u e w_1a são potência de uma mesma palavra, digamos z. Consequentemente,

$$\exists i, j \in \mathbb{N} : \quad u = z^i, \quad w_1a = z^j.$$

Em particular $s_1(u) = s_1(w_1a) = a$, o que é absurdo pois, por hipótese, $s_1(u) \neq a$. Portanto o corolário é verdadeiro. $\square$

Dada uma ordem total sobre o alfabeto A, extende-se esta ordem a uma ordem total sobre A^+, $<_{lex}$, chamada *ordem lexicográfica*, a qual notaremos simplesmente por $<$. Para um par de palavras u, v de A^+ diz-se que $u < v$ se, ou $v \in uA^+$ (uA^+ é aqui considerado como o conjunto de todas as palavras que têm u como prefixo), ou caso existam $a, b \in A$ e $x, y, z \in A^*$ tais que $u = xay$ e $v = xbz$ então $a < b$. Através da definição, é imediato verificar que a ordem lexicográfica possui as seguintes propriedades:

- $\forall u \in A^*,\ v < w \Leftrightarrow uv < uw$,

- $\forall u, v \in A^*,\ w \notin zA^*$ e $z < w \Rightarrow zu < wv$.

Fixada uma ordem lexicográfica sobre A^+, diz-se que uma palavra primitiva $w \in A^+$ é uma palavra de *Lyndon* se

$$\forall u, v \in A^+, \quad w = uv \Rightarrow w < vu.$$

O conjunto de todas as palavras de Lyndon denota-se por *Lyn*.

Exemplo 2.6 *Para $A = \{a, b, c\}$ e $a < b < c$, o conjunto das palavras de Lyndon é (apresentamos apenas as palavras de comprimento menor ou igual a 3)*

$$Lyn = \{a, b, c, ab, ac, bc, aab, aac, abb, abc, acb, acc, bbc, bcc, \ldots\}.$$

Consideremos a palavra $w = bba$. Tomando $u = bb$ e $v = a$ tem-se $w = uv$. Ora $vu = abb < bba = uv = w$ pelo que w não é uma palavra de Lyndon.

2.2 Palavras infinitas

Seja A um alfabeto. Uma *palavra infinita à direita* sobre A é uma sequência $u = u_1u_2u_3\cdots$ de letras u_i indexadas por $\mathbb{N}$, ou seja, é uma aplicação $u : \mathbb{N} \to A$ tal que $u(n) = u_n$. O conjunto de todas as palavras infinitas à direita sobre A representa-se por $A^{\mathbb{N}}$.

A notação $u_{[i,j]}$ $(i, j \in \mathbb{N},\ i \leq j)$ representa o factor (finito) $u_iu_{i+1}\cdots u_j$. O factor $u_{[1,j]}$, diz-se um prefixo (finito) de u e denota-se $p_j(u)$.

O produto de uma palavra finita $u = u_1u_2\cdots u_n$ de A^* por uma palavra infinita à direita $v = v_1v_2\cdots$ de $A^{\mathbb{N}}$ é a palavra infinita à direita

$$uv = u_1u_2\cdots u_nv_1v_2\cdots.$$

Define-se, de forma análoga, *palavra infinita à esquerda* sobre o alfabeto A como uma sucessão u de letras de A indexada por $-\mathbb{N}$, e representa-se $u = \cdots u_{-3}u_{-2}u_{-1}$. O conjunto de todas as palavras infinitas à esquerda sobre A representa-se por $A^{-\mathbb{N}}$.

Mantém-se a notação, $u_{[i,j]}$ $(i, j \in -\mathbb{N},\ i \leq j)$ para representar o factor (finito) $u_iu_{i+1}\cdots u_j$. Neste caso, o factor $u_{[i,-1]}$ diz-se um sufixo (finito) de u e denota-se $s_{-i}(u)$.

A notação Pref(u) (resp. Suf(u)) será utilizada para representar o conjunto dos prefixos (resp. sufixos) de u, com u uma palavra finita ou infinita à direita (resp. esquerda).

O produto de uma palavra infinita à esquerda $v = \cdots v_{-2}v_{-1}$ de $A^{-\mathbb{N}}$ por uma palavra finita $u = u_1u_2\cdots u_n$ de A^* é a palavra infinita à esquerda

$$vu = \cdots v_{-2}v_{-1}u_1u_2\cdots u_n.$$

Consideremos $u = u_1u_2\cdots u_n$ uma palavra de A^+. Para notar a palavra infinita à direita (resp. à esquerda) obtida por repetição infinita à direita (resp. à esquerda) da palavra u, escreve-se $u^{+\infty}$ (resp. $u^{-\infty}$). Tem-se então

$$u^{+\infty} = u_1u_2\cdots u_nu_1u_2\cdots u_n\cdots$$

$$u^{-\infty} = \cdots u_1u_2\cdots u_nu_1u_2\cdots u_n.$$

Seja $p \in \mathbb{N}$ e $w \in A^{\mathbb{N}}$. Se existe um natural r tal que $w_n = w_{n+p}$ para todo o n maior ou igual a r, então p diz-se um período último da palavra infinita à direita w e esta diz-se *ultimamente periódica*. Uma palavra $w \in A^{\mathbb{N}}$ ultimamente periódica é da forma $w = uv^{+\infty}$, com $u \in A^*$ e $v \in A^+$. Note-se que, se $u = 1$ a palavra ultimamente periódica é da forma $w = v^{+\infty}$ e diz-se *periódica*.

Dada uma palavra ultimamente periódica w, chama-se *o período último de* w ao menor dos períodos últimos de w. Se $p_0 \in \mathbb{N}$ é o período último de uma palavra $w \in A^{\mathbb{N}}$, então existe um natural minimal r_0 tal que $w_n = w_{n+p_0}$ para todo o n maior ou igual a r_0. Este natural minimal r_0 é designado o *índice* de w. Assim, a palavra w pode escrever-se na dita *forma canónica*, como

$$w = w_1w_2\cdots w_{r_0-1}(w_{r_0}w_{r_0+1}\cdots w_{r_0+p_0-1})^{+\infty},$$

onde $w_1w_2\cdots w_{r_0-1} \in A^*$ e $w_{r_0}w_{r_0+1}\cdots w_{r_0+p_0-1} \in A^+$. O facto de r_0 ser minimal permite concluir que a letra w_{r_0-1} (se $r_0 > 1$) é diferente da letra $w_{r_0+p_0-1}$. Pelo Corolário 2.5, a palavra w é periódica se e só se $r_0 = 1$. Portanto, para $u, v, w \in A^+$, se $s_1(u) \neq s_1(v)$, uma igualdade do tipo $uv^{+\infty} = w^{+\infty}$ não é possível. Note-se ainda que a palavra $w_{r_0}\cdots w_{r_0+p_0-1}$ é primitiva pelo facto de p_0 ser o período de w.

Exemplo 2.7 *Seja* $w = abcaca^2ca^2ca^2\cdots$ *uma palavra ultimamente periódica. O período último de* w *é* 3*. Pode escrever-se*

$$w = abca(ca^2)^{+\infty} = abc(aca)^{+\infty}.$$

Esta última representação de w *verifica* $s_1(abc) = c \neq a = s_1(aca)$*. Consequentemente, é a sua forma canónica.*

Analogamente, uma palavra $w \in A^{-\mathbb{N}}$ diz-se ultimamente periódica se

$$w = v^{-\infty}u \text{ para alguns } u \in A^* \text{ e } v \in A^+.$$

Se u e v forem escolhidas de comprimento mínimo, então $v^{-\infty}u$ é a forma canónica de w. A palavra w diz-se periódica se u é a palavra vazia.

2.3 Palavras biinfinitas

Define-se *palavra biinfinita pontuada* sobre o alfabeto A, como sendo uma sucessão de letras indexada por $\mathbb{Z}$

$$u = \cdots u_{-2}u_{-1}u_0u_1u_1u_2\cdots,$$

e denota-se $u = (u_i)_{i\in\mathbb{Z}}$. Para indicar qual a letra u_0, fazemos a separação dos u_i com $i \geq 0$ dos u_i com $i < 0$ por um ponto. Por exemplo,

$$u = \cdots ab \cdot cba \cdots$$

significa que $u_{-2} = a, u_{-1} = b, u_0 = c, u_1 = b$ e $u_2 = a$.

O conjunto de todas as palavras biinfinitas pontuadas sobre A representa-se por $A^{\mathbb{Z}}$. Um *factor* de u, com $u \in A^{\mathbb{Z}}$, é uma palavra do tipo $u_{[i,j]} = u_i \cdots u_j$, com $i, j \in \mathbb{Z}$, tal que $i \leq j$. Para representar o conjunto dos factores (resp. de comprimento k) de uma palavra w (finita, infinita ou biinfinita pontuada) escreve--se $Fact(w)$ (resp. $Fact_k(w)$).

Sejam u e v duas palavras infinitas tais que $u \in A^{-\mathbb{N}}$ e $v \in A^{\mathbb{N}}$. De forma natural representaremos por $u \cdot v$ a palavra biinfinita pontuada definida por

$$(u\cdot v)_n = \begin{cases} u_n & \text{se } n \leq -1 \\ v_{n+1} & \text{se } n \geq 0 \end{cases}$$

ou seja, $u \cdot v = \cdots u_{-2}u_{-1} \cdot v_1v_2 \cdots$.

Para cada $n \in \mathbb{Z}$ define-se um *operador de translação* sobre $A^{\mathbb{Z}}$ como sendo a aplicação $\sigma^n : A^{\mathbb{Z}} \longrightarrow A^{\mathbb{Z}}$, definida para cada $u = (u_i)_{i\in\mathbb{Z}}$ por $\sigma^n(u) = (u_{i+n})_{i\in\mathbb{Z}}$.

Diz-se que um par de palavras biinfinitas pontuadas u e v são *similares*, e escreve-se $u \sim v$, se $v = \sigma^n(u)$ para algum $n \in \mathbb{Z}$. Uma *palavra biinfinita* sobre A é uma $\sim$-classe de $A^{\mathbb{Z}}$ e denota-se por $\widetilde{A^{\mathbb{Z}}}$ o conjunto de todas as palavras biinfinitas sobre A.

Tomando $u \in A^{-\mathbb{N}}$ e $v \in A^{\mathbb{N}}$, duas palavras infinitas, uv representa a $\sim$-classe da palavra biinfinita pontuada $u \cdot v$. Por exemplo, considerando $A = \{a, b\}$, a palavra biinfinita sobre o albabeto A

$$b^{-\infty}ab^{+\infty}$$

representa a $\sim$-classe das palavras biinfinitas pontuadas sobre o alfabeto A com uma única ocorrência da letra a.

Uma palavra biinfinita da forma $v^{-\infty}v^{+\infty}$, com $v \in A^+$, denota-se simplesmente por v^{∞} e diz-se *periódica*.

Consideremos uma palavra biinfinita pontuada $w = (w_i)_{i\in\mathbb{Z}}$. Se existe $n \in \mathbb{N}$ tal que $w = \sigma^n(w)$, então w é *periódica*. Sendo u um factor de w de comprimento n, então u diz-se um *período* de w. Portanto, w é determinada por cada um dos seus factores de comprimento n. Assim, também uma palavra biinfinita periódica admite várias representações.

Exemplo 2.8 *A palavra biinfinita associada à palavra biinfinita pontuada* $u = (u_i)_{i\in\mathbb{Z}}$ *tal que* $u_{3n-1} = a$; $u_{3n} = b$ *e* $u_{3n+1} = c$, $n \in \mathbb{Z}$, *pode representar-se nas formas seguintes*

$$\begin{aligned}
\cdots abcabcabc \cdots &= \cdots abcabc(abc)^{+\infty} \\
&= \cdots bcabca(bca)^{+\infty} \\
&= \cdots cabcab(cab)^{+\infty} \\
&= (abc)^{-\infty}abcabc \cdots \\
&= (abc)^{-\infty}abc(abc)^{+\infty} \\
&= (abc)^{\infty} \\
&= etc.
\end{aligned}$$

Seja $w \in A^{\widetilde{\mathbb{Z}}}$ uma palavra biinfinita periódica. Analogamente aos casos infinitos unilaterais, existe uma palavra $u \in A^+$, de comprimento minimal, tal que $w = u^\infty$. A igualdade $w = v^\infty$, é imediata para toda a palavra $v \in A^+$ conjugada de u. Reciprocamente, se $w = z^\infty$, com $z \in A^+$ de comprimento minimal (ou seja, $|z| = |u|$), então z é conjugada de u. Resumindo, se $w = u^\infty$ com u de comprimento minimal, tem-se

$$w = v^\infty, \text{ com } v \in A^+ \text{de comprimento minimal} \Leftrightarrow v \text{ é conjugada de } u.$$

Note-se que fixada uma ordem lexicográfica, existe no conjunto das palavras conjugadas de u uma única palavra de Lyndon x. Em particular tem-se

$$w = x^\infty,$$

que se designa a *forma canónica* de w e x o seu *período.*

Por analogia aos casos infinitos unilaterais, uma palavra biinfinita $w \in A^{\widetilde{\mathbb{Z}}}$ diz-se *ultimamente periódica* se existem $x, z \in A^+$ e $y \in A^*$ tais que

$$w = x^{-\infty} y z^{+\infty}.$$

Seja $w \in A^{\widetilde{\mathbb{Z}}}$. Se w é ultimamente periódica mas não é periódica, então existem $u \in A^+$ de comprimento minimal, $a \in A$ e $r \in A^{\mathbb{N}}$ tais que $w = u^{-\infty} ar$, onde a primeira letra de u é diferente de a. Sendo $s \in A^*$ e $v \in A^+$ tais que $r = sv^{+\infty}$ é a forma canónica de r, a representação

$$w = u^{-\infty} asv^{+\infty}$$

é denominada a *forma canónica* de w.

Exemplo 2.9

Consideremos o alfabeto $A = \{a, b, c\}$ *e* w *a palavra biinfinita sobre* A *tal que,* $w = (cbacbacba)^{-\infty} cbac(abab)^{+\infty}$. *Pode deduzir-se sucessivamente*

$$\begin{aligned} w &= (cbacbacba)^{-\infty} cbac(abab)^{+\infty} \\ &= ((\underline{cba})^3)^{-\infty} \underline{cba}\, c((ab)^2)^{+\infty} \\ &= (cba)^{-\infty} c(ab)^{+\infty} \\ &= (cba)^{-\infty} c\, \underline{a}\, b(ab)^{+\infty} \\ &= (bac)^{-\infty} \underline{a}\, (ba)^{+\infty}. \end{aligned}$$

Consideremos agora, $w' = (c^2ab)^{-\infty}c^2abc(cabc^2abc)^{+\infty}$. *Então*

$$\begin{aligned} w' &= (c^2ab)^{-\infty}c^2abc(cabc^2abc)^{+\infty} \\ &= (cabc)^{-\infty}cabc((cabc)^2)^{+\infty} \\ &= (cabc)^{-\infty}(cabc)^{+\infty} \\ &= (cabc)^{\infty} \\ &= (abc^2)^{\infty}. \end{aligned}$$

2.4 Factores das palavras biinfinitas

Note-se que, se $w, z \in A^{\mathbb{Z}}$ são palavras similares, então $Fact(w) = Fact(z)$. Portanto as definições e notações, respeitantes a factores, introduzidas para palavras biinfinitas pontuadas podem ser extendidas de forma natural às palavras biinfinitas.

O teorema seguinte é um resultado clássico de combinatória de palavras.

Teorema 2.10 ([32]) *Seja w uma palavra biinfinita. Se a partir de uma certa ordem k, com $k \in \mathbb{N}$, $|Fact_{k+1}(w)| = |Fact_k(w)|$, então w é periódica.*

Podemos agora provar alguns lemas (retirados de [21]) que serão úteis mais tarde.

Lema 2.11 *Sejam $w, z \in A^{\widetilde{\mathbb{Z}}}$ um par de palavras biinfinitas ultimamente periódicas tais que $Fact(w) \subseteq Fact(z)$.*

1. *Se z é periódica, então $w = z$.*

2. *Se z não é periódica e a sua forma canónica é do tipo $z = x^{-\infty}auy^{+\infty}$, com $x, y \in A^+$, $a \in A$ e $u \in A^*$, então tem-se $w = z$, $w = x^{\infty}$ ou $w = y^{\infty}$.*

Demonstração: Comecemos por supor que z é periódica, i.e., que existe $u \in A^+$ tal que $z = u^{\infty}$.

Por hipótese $Fact(w) \subseteq Fact(z)$, e consequentemente, para todo o $n \in \mathbb{N}$ verifica-se $|Fact_n(w)| \leq |Fact_n(z)|$. Como $z = u^{\infty}$, então para todo o $n \in \mathbb{N}$ tem-se que $|Fact_n(z)| \leq |u|$. Portanto, a sucessão $(|Fact_n(w)|)_{n\in\mathbb{N}}$ é limitada. Tendo em consideração que $(|Fact_n(w)|)_{n\in\mathbb{N}}$ é uma sucessão monótona crescente, é imediato concluir que a sucessão $(|Fact_n(w)|)_{n\in\mathbb{N}}$ é convergente. Assim, existe

$j \in \mathbb{N}$ tal que $|Fact_{j+1}(w)| = |Fact_j(w)|$ o que, pelo Teorema 2.10, permite concluir que w é periódica.

Consideremos então que $w = v^\infty$ para alguma palavra $v \in A^+$. Em particular, para todo o inteiro $k \in \mathbb{N}$, v^k é factor de z, pois v^k é factor de w e $Fact(w) \subseteq Fact(z)$. Então, se escolhermos $k \in \mathbb{N}$ tal que

$$|v^k| \geq |v| + |u| - mdc(|v|, |u|),$$

existem $r \in A^+$ conjugada de u, $r' \in A^*$ prefixo próprio de r e um inteiro $m \in \mathbb{N}$ tais que

$$v^k = r^m r'.$$

Pela Proposição 2.4, deduz-se que v e r são potências de uma mesma palavra, digamos t. Portanto, $v^\infty = t^\infty = r^\infty$. Como r é conjugada de u, então $r^\infty = u^\infty$. Consequentemente,

$$w = v^\infty = t^\infty = r^\infty = u^\infty = z.$$

Suponhamos agora que z não é periódica e seja $z = x^{-\infty}auy^{+\infty}$ a sua forma canónica, onde $x, y \in A^+$, $a \in A$, $u \in A^*$ e $p_1(x) \neq a$. Temos então uma das seguintes situações:

- w é periódica, isto é, existe $r \in A^+$ tal que $w = r^\infty$. Então r^k é factor de z, para todo o $k \in \mathbb{N}$. Como o comprimento de au é finito, tem-se que r^k é factor de $x^{-\infty}$ ou de $y^{+\infty}$. Suponhamos que r^k é factor de $x^{-\infty}$. Então, se escolhermos k suficientemente grande, tal que

  $$|r^k| \geq |r| + |x| - mdc(|r|, |x|),$$

  através de um raciocínio análogo ao usado na demonstração do ponto 1 conclui-se que

  $$w = r^\infty = x^\infty.$$

  Analogamente, se r^k é factor de $y^{+\infty}$, então $w = y^\infty$.

- w não é periódica e admite como forma canónica $w = x_1^{-\infty}a_1u_1y_1^{+\infty}$, onde $x_1, y_1 \in A^+$, $a_1 \in A$, $u_1 \in A^*$ e a primeira letra de x_1 é distinta de a_1.
  Por hipótese, $x_1^k a_1$ é factor de z para todo o $k \in \mathbb{N}$. Em particular, para k suficientemente grande, deduzimos do Corolário 2.5 que $x_1^k a_1$ não é factor

de x^p nem de y^p, qualquer que seja $p \in \mathbb{N}$. Portanto $x_1^k a_1$ tem uma única ocorrência em z. Mais precisamente, $x_1^k a_1$ é sufixo de $x^{-\infty}a$. Note-se que se este não fosse o caso, teriamos para todo o $n \in \mathbb{N}$, $x_1^n a_1$ factor de $y^{+\infty}$, ou $x^n a$ como factor de uma potência de x_1, o que pelo Corolário 2.5 não é possível.

Como $x_1^k a_1$ é sufixo de $x^{-\infty}a$ para todo o k então, para todo o $r \in \mathbb{N}$,

$$s_r(x_1^{-\infty}a_1) = s_r(x^{-\infty}a),$$

e portanto, $x_1^{-\infty}a_1 = x^{-\infty}a$.
Tem-se ainda que para k suficientemente grande verifica-se também que a palavra $x_1^k a_1 p_k(u_1 y_1^{+\infty})$ é um factor de z com uma única ocorrência. Deduz--se assim que $p_k(u_1 y_1^{+\infty}) = p_k(uy^{+\infty})$ e consequentemente, $u_1 y_1^{+\infty} = uy^{+\infty}$. Tendo em consideração que $x_1^{-\infty}a_1 = x^{-\infty}a$ e $u_1 y_1^{+\infty} = uy^{+\infty}$, podemos concluir que

$$w = x_1^{-\infty}a_1 u_1 y_1^{+\infty} = x^{-\infty}auy^{+\infty} = z.$$

□

Lema 2.12 *Sejam w e z um par de palavras ultimamente periódicas tais que $w \in A^{\widetilde{\mathbb{Z}}}$ e $z = uv^{+\infty} \in A^{\mathbb{N}}$ (resp. $z = v^{-\infty}u \in A^{-\mathbb{N}}$), com $u \in A^*$ e $v \in A^+$. Se $Fact(w) \subseteq Fact(z)$, então $w = v^{\infty}$.*

Demonstração: Dado que $Fact(w) \subseteq Fact(z)$, então

- se $u = 1$ (donde $z = v^{\infty}$), z é periódica e pelo ponto 1 do lema anterior $w = z = v^{\infty}$.
- se $u \neq 1$, $z = uv^{+\infty}$. Como por hipótese $Fact(w) \subseteq Fact(uv^{+\infty})$, também $Fact(w) \subseteq Fact(r^{-\infty}uv^{+\infty})$ para todo o $r \in A^+$. Consequentemente, como w é uma palavra fixa de $A^{\widetilde{\mathbb{Z}}}$ e pelo ponto 2 do lema anterior, conclui-se que $w = v^{\infty}$. □

Dado um conjunto B de palavras, denota-se $Fact(B) = \bigcup_{w\in B} Fact(w)$.

Lema 2.13 *Seja $w \in A^{\widetilde{\mathbb{Z}}}$ uma palavra biinfinita e seja B um subconjunto finito de $A^{\mathbb{N}} \cup A^{-\mathbb{N}} \cup A^{\widetilde{\mathbb{Z}}}$. Se $Fact(w) \subseteq Fact(B)$, então existe $z \in B$ tal que $Fact(w) \subseteq Fact(z)$.*

Demonstração: Consideremos $x = (x_i)_{i \in \mathbb{Z}}$ uma palavra biinfinita pontuada representante de w. Para todo o $k \in \mathbb{N}$, $x_{[-k,k]}$ é factor de w, pois $Fact(x) = Fact(w)$. Por hipótese $Fact(w) \subseteq Fact(B)$, e portanto $x_{[-k,k]} \in Fact(B)$. Como B é finito e $x_{[-n,n]}$ é factor de $x_{[-k,k]}$, para todos os $n, k \in \mathbb{N}$ tais que $n \leq k$, então existe uma palavra $z \in B$ tal que $x_{[-k,k]}$ é factor de z para todo o $k \in \mathbb{N}$. Conclui-se assim que $Fact(w) \subseteq Fact(z)$. □

Capítulo 3

Variedades

3.1 Variedades de semigrupos

O conceito de variedade de semigrupos deve-se a Birkhoff. Para a introdução deste conceito comecemos por referir alguns *operadores* sobre as classes de semigrupos. Fixemos uma classe $\mathcal{C}$ de semigrupos. Denota-se,

- $H(\mathcal{C})$ a classe das imagens homomorfas dos semigrupos de $\mathcal{C}$;
- $S(\mathcal{C})$ a classe dos subsemigrupos de semigrupos de $\mathcal{C}$;
- $P(\mathcal{C})$ a classe dos produtos directos de semigrupos de $\mathcal{C}$.

Uma classe não vazia de semigrupos, $\mathcal{V}$, diz-se uma *variedade* se ela é fechada para os operadores H, S e P. Como uma variedade de semigrupos é fechada para a formação de subsemigrupos e imagens homomorfas, então é fechada para a divisão. Portanto, $\mathcal{V}$ é uma variedade se é fechada para a divisão e para produtos directos. Como exemplos de classes de semigrupos que formam variedades tem-se:

- $\mathcal{S}$, a classe de todos os semigrupos;
- $\mathcal{S}l$, a classe de todos os semi-reticulados.

Toda a intersecção de variedades é ainda uma variedade. Podemos portanto definir a variedade *gerada* por uma classe $\mathcal{C}$ de semigrupos, denotada por $V(\mathcal{C})$, como sendo a intersecção de todas as variedades que contêm $\mathcal{C}$.

Mais geralmente, uma dada classe de álgebras do mesmo tipo τ diz-se uma τ--variedade se ela é fechada para os operadores H, S e P (cuja definição é adaptada daquela dada inicialmente: basta substituir semigrupos por álgebras do tipo τ).

3.1.1 Identidades para variedades

Seja A um alfabeto. Uma *identidade* sobre A é um par (u, v) de palavras de A^+, normalmente representada pela igualdade formal $u = v$. Uma identidade da forma $u = u$ diz-se *trivial*.

Diz-se que um semigrupo S *verifica* ou *satisfaz* a identidade $u = v$, e escreve-se $S \models u = v$, se para qualquer homomorfismo $\varphi : A^+ \to S$, $\varphi(u) = \varphi(v)$.

Uma classe $\mathcal{C}$ de semigrupos satisfaz um conjunto Σ de identidades, e denota--se $\mathcal{C} \models \Sigma$, se

$$\forall S \in \mathcal{C}\ \forall u = v \in \Sigma,\ S \models u = v.$$

Dado um conjunto Σ de identidades, verifica-se que a classe de todos os semigrupos que satisfazem todas as identidades de Σ é uma variedade. A notação $[\Sigma]$ é utilizada para representar essa variedade.

Uma classe de semigrupos $\mathcal{V}$ diz-se *equacional* se existe um conjunto Σ de identidades tal que $\mathcal{V} = [\Sigma]$. Neste caso, diz-se que Σ é uma *base (de identidades)* de $\mathcal{V}$.

O resultado fundamental seguinte, enunciado apenas para semigrupos, foi demonstrado em 1935 por Birkhoff para classes de álgebras do mesmo tipo.

Teorema 3.1 (Birkhoff) *Uma classe de semigrupos é uma variedade se e só se ela é equacional.*

Fixemos agora uma identidade $u = v$ e um conjunto Σ de identidades sobre A.

Denota-se por $\Sigma \models u = v$, e diz-se que Σ implica $u = v$, se para todo o semigrupo S, $S \models \Sigma$ implica $S \models u = v$.

Vejamos como obter "construtivamente" $u = v$ a partir de Σ.

Chama-se *fecho dedutivo* de Σ ao menor conjunto $D(\Sigma)$ de identidades sobre A tal que $\Sigma \subseteq D(\Sigma)$ e:

1. $u = u \in D(\Sigma)$, para todo o $u \in A^+$;

2. $u = v \in D(\Sigma) \Rightarrow v = u \in D(\Sigma)$;

3. $u = v, v = w \in D(\Sigma) \Rightarrow u = w \in D(\Sigma)$;

4. $u = v \in D(\Sigma), r, s \in A^* \Rightarrow rus = rvs \in D(\Sigma)$;

5. $u = v \in D(\Sigma), a \in A, r \in A^+ \Rightarrow u' = v' \in D(\Sigma)$, onde u' e v' são as palavras obtidas a partir das palavras u e v, respectivamente, pela substituição de cada ocorrência de a por r.

Dizemos por fim que $u = v$ é *dedutível* das identidades de Σ, e escrevemos $\Sigma \vdash u = v$, se existir uma dedução de $u = v$ a partir de Σ, i.e., uma sucessão finita

$$u_1 = v_1, u_2 = v_2, \ldots, u_n = v_n$$

de identidades sobre A, tais que, cada $u_i = v_i$ pertence a Σ, ou é da forma $u = u$ ou é obtida de identidades que a precedem na sucessão, usando uma das transformações indicadas em 2 a 5, e $u_n = v_n$ é a identidade $u = v$.

O teorema seguinte apesar de ser aqui enunciado apenas para semigrupos pode ser enunciado para quaisquer classes de álgebras do mesmo tipo.

Teorema 3.2 (Completude da lógica equacional-Birkhoff) *Sejam Σ e $u = v$, respectivamente, um conjunto de identidades e uma identidade de semigrupos sobre A. As condições seguintes são equivalentes :*

1. $\Sigma \models u = v$;

2. $\Sigma \vdash u = v$;

3. $u = v \in D(\Sigma)$.

3.2 Pseudovariedades de semigrupos

Para as classes de semigrupos finitos dispomos de um conceito análogo ao de variedade definido na secção anterior para semigrupos quaisquer. Trata-se do conceito de pseudovariedade introduzido por Eilenberg em 1976.

Uma *pseudovariedade* de semigrupos é uma classe não vazia, $\mathbf{V}$, de semigrupos finitos, tal que:

i) se $S \in \mathbf{V}$ e $T \leq S$, então $T \in \mathbf{V}$;

ii) se $S \in \mathbf{V}$ e $\varphi : S \to T$ é um epimorfismo de semigrupos, então $T \in \mathbf{V}$;

iii) se $S_1, \ldots, S_n \in \mathbf{V}$, então $S_1 \times \cdots \times S_n \in \mathbf{V}$.

De forma equivalente, $\mathbf{V}$ é uma pseudovariedade de semigrupos se é fechada para a divisão e para produtos directos finitos. Como exemplos de classes de semigrupos finitos que formam pseudovariedades podemos referir:

- **S**, a classe de todos os semigrupos finitos;
- **I**, a classe constituída pelos semigrupos com um único elemento, chamada a *pseudovariedade trivial*;
- **Sl**, a classe de todos os semi-reticulados finitos;
- **G**, a classe de todos os grupos finitos;
- **N**, a classe de todos os semigrupos nilpotentes finitos;
- **K**, a classe de todos os semigrupos finitos S tais que $es = e$ para todos os $e \in E(S)$ e $s \in S$;
- **D**, a classe de todos os semigrupos finitos S tais que $se = e$ para todos os $e \in E(S)$ e $s \in S$;
- **LI**, a classe de todos os semigrupos finitos localmente triviais.

Refira-se também as pseudovariedades definidas pelas relações de Green. Prova-se que, se $\mathcal{K}$ é uma das relações de Green, então a classe dos semigrupos finitos $\mathcal{K}$-triviais é uma pseudovariedade. Se $\mathcal{K}$ é $\mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$ ou $\mathcal{H}$, a pseudovariedade dos semigrupos finitos $\mathcal{K}$-triviais correspondente é representada por **R**, **L**, **J** e **A**.

Pelo contrário, as seguintes classes não constituem pseudovariedades:

- A classe de todos os semigrupos regulares finitos;
- A classe de todos os semigrupos inversos finitos.

Para esta última tem-se, por exemplo, o semigrupo B_2 do Exemplo 1.16 que pertence à classe de todos os semigrupos inversos finitos, no entanto, se considerarmos $T = B_2 \backslash \{b\}$ verifica-se que T é um subsemigrupo de B_2 mas não é um semigrupo inverso, pois a não tem inverso em T. Portanto falha a condição $i)$ da definição de pseudovariedade.

A intersecção de pseudovariedades é ainda uma pseudovariedade. Em particular, se considerarmos uma classe de semigrupos finitos $\mathcal{C}$, define-se a pseudovariedade gerada por $\mathcal{C}$ como sendo a intersecção de todas as pseudovariedades que contêm $\mathcal{C}$, denotando-a por $\mathbf{V}(\mathcal{C})$. A pseudovariedade $\mathbf{V}(\mathcal{C})$ pode ainda ser definida de uma forma construtiva por:

$$\mathbf{V}(\mathcal{C}) = \{S \in \mathbf{S} : \exists n \in \mathbb{N}\ \exists S_1, \ldots, S_n \in \mathcal{C},\ S \prec S_1 \times \ldots \times S_n\}.$$

No caso de $\mathcal{C}$ ser formada apenas por um semigrupo S, escreve-se simplesmente $\mathbf{V}(S)$ para designar a pseudovariedade gerada por $\mathcal{C}$, que também é designada por *pseudovariedade gerada por S*.

Seja $\mathbf{V}$ uma pseudovariedade. O conjunto das pseudovariedades contidas em $\mathbf{V}$, ditas *subpseudovariedades* de $\mathbf{V}$, denota-se por $\mathcal{P}_S\mathbf{V}$. O par $(\mathcal{P}_S\mathbf{V}, \subseteq)$ é um reticulado e dadas duas pseudovariedades $\mathbf{V}$ e $\mathbf{W}$ de $\mathcal{P}_S\mathbf{S}$,

- o *ínfimo* $\mathbf{V} \wedge \mathbf{W}$ é a intersecção $\mathbf{V} \cap \mathbf{W}$;
- o *supremo* $\mathbf{V} \vee \mathbf{W}$ é a pseudovariedade gerada pela união $\mathbf{V} \cup \mathbf{W}$.

De facto $\mathbf{V} \cap \mathbf{W}$ é uma pseudovariedade para todos os $\mathbf{V}$ e $\mathbf{W}$, enquanto que $\mathbf{V} \cup \mathbf{W}$ é uma pseudovariedade se e só se $\mathbf{V} \subseteq \mathbf{W}$ ou $\mathbf{W} \subseteq \mathbf{V}$.

O cálculo da intersecção de duas pseudovariedades $\mathbf{V}$ e $\mathbf{W}$ não coloca grandes dificuldades. Se $\mathbf{V} = [\![\Sigma_1]\!]$ e $\mathbf{W} = [\![\Sigma_2]\!]$, então

$$\mathbf{V} \cap \mathbf{W} = [\![\Sigma_1 \cup \Sigma_2]\!].$$

A notação $[\![\Sigma]\!]$ será introduzida na secção 3.2.3.

Pelo contrário, o cálculo de $\mathbf{V} \vee \mathbf{W}$ é muito complexo em geral e este problema ainda está relativamente pouco estudado.

3.2.1 Identidades para pseudovariedades

Seja Σ um conjunto de identidades. A classe de todos os semigrupos finitos que verificam todas as identidades de Σ é uma pseudovariedade. Denota-se essa pseudovariedade por $[\![\Sigma]\!]$ e dizemos que é *definida* por Σ.

Uma pseudovariedade $\mathbf{V}$ diz-se *equacional* se existe um conjunto Σ de identidades tal que $\mathbf{V} = [\![\Sigma]\!]$. Neste caso, diz-se que Σ é uma *base de identidades* de $\mathbf{V}$. As pseudovariedades seguintes são equacionais

$$\mathbf{S} = [\![a = a]\!],\ \mathbf{I} = [\![a = b]\!],\ \mathbf{B} = [\![a = a^2]\!],\ \mathbf{Sl} = [\![ab = ba, a = a^2]\!].$$

Pelo contrário, as pseudovariedades $\mathbf{G}$ e $\mathbf{N}$ não satisfazem identidades não triviais (a demonstração desta propriedade de $\mathbf{N}$ será provada na Proposição 4.5). Portanto tem-se o seguinte resultado.

Proposição 3.3 *Toda a pseudovariedade, distinta de* $\mathbf{S}$*, contendo* $\mathbf{G}$ *ou* $\mathbf{N}$ *é não equacional.*

Como já referimos, nem todas as pseudovaridades são equacionais. No entanto, todas podem ser definidas ultimamente através de identidades, como mostra o teorema seguinte.

Teorema 3.4 (Eilenberg-Schützenberger [24]) *Uma classe não vazia* $\mathcal{U}$ *de semigrupos finitos é uma pseudovariedade se e só se existe uma sucessão* $(u_n = v_n)_{n\in\mathbb{N}}$ *de identidades tal que*

$$\mathcal{U} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash u_n = v_n\}.$$

Ou seja, $\mathcal{U}$ *é constituída pelos semigrupos finitos que satisfazem todas as identidades* $u_n = v_n$*, a partir de uma certa ordem. Dizemos nesse caso, que* $\mathcal{U}$ *é definida ultimamente pela sucessão* $(u_n = v_n)_{n\in\mathbb{N}}$*.*

Como exemplos, apresentamos:

- $\mathbf{G} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash a^{n!}b = ba^{n!} = b\}$;
- $\mathbf{N} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash a^n b = ba^n = a^n\}$;
- $\mathbf{R} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash (ab)^n = (ab)^n a\}$;

- $\mathbf{J} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\, \forall n \geq p,\ S \models (ab)^n a = (ab)^n = b(ab)^n\}$.

Esta notação pode ser bastante simplificada se utilizarmos pseudoidentidades, que passaremos a definir, em vez de identidades. Comecemos por introduzir a noção de operação implícita.

3.2.2 Operações implícitas

Seja $\mathbf{V}$ uma pseudovariedade e seja $A = \{a_1, \ldots, a_n\}$ um alfabeto de cardinalidade $n \in \mathbb{N}$. Uma *operação ímplicita* A-ária (ou n-ária) sobre $\mathbf{V}$ é uma família $\pi = (\pi_S)_{S\in\mathbf{V}}$ tal que

- para cada $S \in \mathbf{V}$, $\pi_S : S^n \to S$ é uma função;
- para qualquer homomorfismo $\varphi : S \to T$ com $S, T \in \mathbf{V}$, o seguinte diagrama comuta

$$\begin{tikzcd} S^n \arrow[r, "\pi_S"] \arrow[d, "\varphi^n"'] & S \arrow[d, "\varphi"] \\ T^n \arrow[r, "\pi_T"] & T \end{tikzcd}$$

Denotaremos o conjunto de todas as operações implícitas A-árias sobre $\mathbf{V}$ por $\overline{\Omega}_A\mathbf{V}$ (ou $\overline{\Omega}_n\mathbf{V}$). Munido da operação binária definida para $\pi, \rho \in \overline{\Omega}_A\mathbf{V}$, $S \in \mathbf{V}$ e $s_1, s_2, \ldots, s_n \in S$, por

$$(\pi \cdot \rho)_S(s_1, \ldots, s_n) = \pi_S(s_1, \ldots, s_n) \cdot \rho_S(s_1, \ldots, s_n)$$

o conjunto $\overline{\Omega}_A\mathbf{V}$ forma um semigrupo.

Como exemplos, os mais simples, de operações implícitas sobre $\mathbf{V}$ temos as operações explícitas que passamos a definir.

Para cada $i \in \{1, \ldots, n\}$, a_i designa-se a *projecção sobre a i-ésima componente* e é definida para $S \in \mathbf{V}$, como sendo a aplicação

$$\begin{array}{rccc} (a_i)_S : & S^n & \to & S \\ & (s_1, \ldots, s_n) & \mapsto & s_i \end{array}$$

O subsemigrupo de $\overline{\Omega}_A\mathbf{V}$ gerado pelo conjunto das projecções $\{a_1, \ldots, a_n\}$ denota-se por $\Omega_A\mathbf{V}$ (ou $\Omega_n\mathbf{V}$) e os seus elementos dizem-se operações *explícitas* A-árias (ou n-árias) sobre $\mathbf{V}$.

Refira-se que as operações explícitas n-árias são operações implícitas n-árias induzidas pelas palavras de A^+. Por exemplo, se $A = \{a_1, a_2, a_3\}$, a palavra finita $u = a_3a_1^2a_2$ define uma operação explícita 3-ária sobre $\mathbf{V}$ (em particular, esta é também uma operação implícita 3-ária sobre $\mathbf{V}$). Para $S \in \mathbf{V}$ podemos definir a aplicação $u_S : S^3 \to S$ para cada $(s_1, s_2, s_3) \in S^3$, por

$$\begin{aligned} u_S(s_1, s_2, s_3) &= (a_3)_S(s_1, s_2, s_3)(a_1)_S(s_1, s_2, s_3)^2(a_2)_S(s_1, s_2, s_3) \\ &= s_3s_1^2s_2. \end{aligned}$$

Note-se que uma operação implícita m-ária pode também ser vista como uma operação implícita n-ária com $n \geq m$. Por exemplo, a palavra $u = a_3a_1^2a_2$ pode ainda ser interpretada como uma operação implícita n-ária, mesmo que n seja maior do que 3.

$$\begin{array}{rccc} (a_3a_1^2a_2)_S : & S^n & \to & S \\ & (s_1, \ldots, s_n) & \mapsto & s_3s_1^2s_2 \end{array}$$

Vejamos um outro exemplo importante de operação implícita.

Designa-se por ω-potência, e denota-se a^ω, a operação implícita unária sobre $\mathbf{V}$ que se define de seguida. Recorde-se que para um semigrupo finito S e $s \in S$, existe exactamente um idempotente da forma s^k, com $k \geq 1$, que se denota por s^ω. A ω-potência é a operação implícita a^ω definida por

$$\begin{array}{rccc} (a^\omega)_S : & S & \to & S \\ & s & \mapsto & s^\omega \end{array}$$

onde $S \in \mathbf{V}$.

Verifiquemos que de facto $\varphi(s^\omega) = \varphi(s)^\omega$, para todo o $s \in S$ e para todo o homomorfismo $\varphi : S \to T$. Como s^ω é idempotente e φ é um homomorfismo, então

$$\varphi(s^\omega) = \varphi(s^\omega \cdot s^\omega) = \varphi(s^\omega) \cdot \varphi(s^\omega),$$

donde se conclui que $\varphi(s^\omega)$ é idempotente. Pela Proposição 1.10, existe $n \in \mathbb{N}$ tal que para todo o $s \in S$, $s^\omega = s^n$. Assim, e tendo em consideração que φ é um homomorfismo obtém-se

$$\varphi(s^\omega) = \varphi(s^n) = \varphi(s \cdots s) = \varphi(s) \cdots \varphi(s) = \varphi(s)^n$$

Portanto, $\varphi(s)^n$ é idempotente, e consequentemente $\varphi(s^\omega) = \varphi(s)^\omega$.

Apesar de usualmente ser uma operação não explícita, a^ω pode, no caso de algumas pseudovariedades, coincidir com operações explícitas sobre $\mathbf{V}$, como verificaremos mais à frente.

Uma operação implícita que pode ser obtida a partir das projecções $a_1, \ldots, a_n$ usando um número finito de vezes as operações de multiplicação e ω-potência é denominada uma *ω-palavra*. O conjunto

$$\Omega_A^\omega \mathbf{V} = \{\pi \in \overline{\Omega}_A \mathbf{V} |\ \pi \text{ é uma } \omega - \text{palavra}\}$$

é um subsemigrupo de $\overline{\Omega}_A \mathbf{V}$.

Note-se que, se $\pi = (\pi_S)_{S \in \mathbf{V}}$ é uma operação implícita sobre $\mathbf{V}$ e $\mathbf{W}$ é uma pseudovariedade contida em $\mathbf{V}$, então $(\pi_S)_{S \in \mathbf{W}}$ é uma operação implícita sobre $\mathbf{W}$ que denotaremos por $q_{\mathbf{V},\mathbf{W}}(\pi)$. A aplicação

$$\begin{array}{rccc} q_{\mathbf{V},\mathbf{W}} : & \overline{\Omega}_A \mathbf{V} & \to & \overline{\Omega}_A \mathbf{W} \\ & (\pi_S)_{S \in \mathbf{V}} & \mapsto & (\pi_S)_{S \in \mathbf{W}} \end{array}$$

será assim designada de *projecção natural* de $\overline{\Omega}_A \mathbf{V}$ sobre $\overline{\Omega}_A \mathbf{W}$. No caso de $\mathbf{V}$ ser a pseudovariedade $\mathbf{S}$, usaremos a notação simplificada $q_{\mathbf{W}}$ para designar $q_{\mathbf{S},\mathbf{W}}$.

Consideremos uma pseudovariedade de semigrupos $\mathbf{V}$. A noção de conteúdo pode agora ser extendida aos elementos de $\overline{\Omega}_A \mathbf{V}$. Tal trabalho é devido a Azevedo [17].

Dizemos que $\pi \in \overline{\Omega}_A \mathbf{V}$ depende de a_i se existem $S \in \mathbf{V}$ e elementos $s_1, \ldots, s_{i-1}$, r, r', $s_{i+1}, \ldots, s_n \in S$ tais que

$$\pi_S(s_1, \ldots, s_{i-1}, r, s_{i+1}, \ldots, s_n) \neq \pi_S(s_1, \ldots, s_{i-1}, r', s_{i+1}, \ldots, s_n),$$

ou seja, a função $\pi_S : S^n \longrightarrow S$ depende da i-ésima componente. O conjunto de todos os a_i dos quais π depende, designa-se o *conteúdo* de π e denota-se por $c(\pi)$.

Lema 3.5 (Azevedo [17]) *Sejam $\mathbf{V}$ uma pseudovariedade qualquer e $\pi \in \overline{\Omega}_A \mathbf{V}$. Se $a_i \in c(\pi)$, então existem $\pi_1, \pi_2 \in (\overline{\Omega}_A \mathbf{V})^1$ tais que $\pi = \pi_1 a_i \pi_2$.*

No caso de $\mathbf{V}$ ser uma pseudovariedade que contém $\mathbf{Sl}$ veremos mais tarde que a aplicação conteúdo, c, coincide com a projecção $q_{\mathbf{V},\mathbf{Sl}}$ de $\overline{\Omega}_A \mathbf{V}$ sobre $\overline{\Omega}_A \mathbf{Sl}$.

Em $\overline{\Omega}_A\mathbf{V}$ pode ser definida uma estrutura topológica, conforme o breve resumo que se segue. Para mais informação sobre a estrutura topológica de $\overline{\Omega}_A\mathbf{V}$ e as suas propriedades métricas, consultar em [4] o subcapítulo 3.4.

Para cada semigrupo $S \in \mathbf{V}$, existe uma aplicação natural

$$\begin{array}{rccc} \alpha_S : & \overline{\Omega}_A\mathbf{V} & \rightarrow & S^{S^n} \\ & \pi & \mapsto & \pi_S \end{array}$$

que induz uma aplicação injectiva

$$\begin{array}{rccc} \alpha_{\mathbf{V}} : & \overline{\Omega}_A\mathbf{V} & \rightarrow & \prod_{S\in\mathbf{V_0}} S^{S^n} \\ & \pi & \mapsto & (\pi_S)_S \end{array}$$

onde $\mathbf{V_0}$ é um conjunto numerável que contém um representante de cada classe de isomorfismo dos elementos de $\mathbf{V}$. Podemos então interpretar $\overline{\Omega}_A\mathbf{V}$ como um subsemigrupo de $\prod_{S\in\mathbf{V_0}} S^{S^n}$.

Consideremos agora os semigrupos finitos munidos da topologia discreta, o produto cartesiano $\prod_{S\in\mathbf{V_0}} S^{S^n}$ munido da topologia produto e $\overline{\Omega}_A\mathbf{V}$ como um subespaço topológico de $\prod_{S\in\mathbf{V_0}} S^{S^n}$ através da aplicação $\alpha_{\mathbf{V}}$.

Proposição 3.6 (Almeida [4]) *Com as definições acima, $\overline{\Omega}_A\mathbf{V}$ é um semigrupo topológico compacto no qual o subespaço $\Omega_A\mathbf{V}$ é denso.*

A topologia de $\overline{\Omega}_A\mathbf{V}$ pode ainda ser vista como a topologia induzida por uma distância d, que descrevemos de seguida.

Seja r a aplicação de $\overline{\Omega}_A\mathbf{V} \times \overline{\Omega}_A\mathbf{V}$ sobre $\mathbb{N}_0 \cup \{+\infty\}$ definida por

$$r(\pi,\rho) = min\{|S| \ : S \in \mathbf{V},\ \pi_S \neq \rho_S\}$$

onde, por convenção, tomamos $min\ \emptyset = +\infty$. Definimos agora uma distância d sobre $\overline{\Omega}_A\mathbf{V}$ fazendo

$$\begin{array}{rccc} d : & \overline{\Omega}_A\mathbf{V} \times \overline{\Omega}_A\mathbf{V} & \rightarrow & \mathbb{R}_0^+ \\ & (\pi,\rho) & \mapsto & \left\{ \begin{array}{cl} 2^{-r(\pi,\rho)} & \text{se } r(\pi,\rho) \text{ é finito} \\ 0 & \text{se } r(\pi,\rho) = +\infty \end{array} \right. \end{array}$$

Pode verificar-se que esta aplicação d é mesmo uma ultramétrica.

Proposição 3.7 (Almeida [4]) *A topologia anteriormente definida sobre $\overline{\Omega}_A\mathbf{V}$ é induzida por d.*

Proposição 3.8 (Almeida [4]) *O espaço métrico $(\overline{\Omega}_A\mathbf{V}, d)$ é o completado do subespaço $(\Omega_A\mathbf{V}, d)$.*

Tendo em consideração o que foi exposto, e uma vez que a convergência de sucessões de operações implícitas será estudada posteriormente, segue com particular interesse a observação seguinte.

Observação 3.9 *Uma sucessão $(\pi_n)_{n\in\mathbb{N}}$ de operações implícitas A-árias sobre $\mathbf{V}$ converge para $\pi \in \overline{\Omega}_A\mathbf{V}$ se e só se, para todo o $S \in \mathbf{V}$, $\pi_S = (\pi_n)_S$, a partir de uma certa ordem, isto é, se e só se a sucessão $(\pi_n)_{n\in\mathbb{N}}$ coincide ultimamente com π em cada $S \in \mathbf{V}$.*

Por exemplo, o limite da sucessão de operações explícitas $(a^{n!})_{n\in\mathbb{N}}$ sobre $\mathbf{V}$ é a operação implícita a^ω sobre $\mathbf{V}$. De facto, para cada semigrupo $S \in \mathbf{V}$ e cada elemento $s \in S$, $s^{n!}$ coincide com o idempotente s^ω para todo o $n \geq |S|$.

3.2.3 Definição de pseudovariedades por pseudoidentidades

Estamos agora em condições de extender a noção de identidade à noção de pseudoidentidade.

Chama-se *pseudoidentidade* sobre $\mathbf{V}$ a um par (π, ρ) de elementos de $\overline{\Omega}_A\mathbf{V}$, a qual é normalmente representada pela igualdade $\pi = \rho$. Diz-se que um semigrupo $S \in \mathbf{V}$ *verifica* ou *satisfaz* a pseudoidentidade $\pi = \rho$, e escreve-se $S \models \pi = \rho$, se for verificada a igualdade de funções $\pi_S = \rho_S$, ou seja, se

$$\pi_S(s_1, \ldots, s_n) = \rho_S(s_1, \ldots, s_n), \text{ para qualquer } (s_1, \ldots, s_n) \in S^n.$$

Uma classe $\mathcal{C}$ de semigrupos de $\mathbf{V}$ *satisfaz* um conjunto Σ de pseudoidentidades, e denota-se $\mathcal{C} \models \Sigma$, se qualquer semigrupo S de $\mathcal{C}$ satisfaz qualquer pseudoidentidade de Σ.

Da mesma forma que para as identidades, se Σ é um conjunto de pseudoidentidades sobre $\mathbf{V}$, a subclasse de $\mathbf{V}$ definida por Σ é uma pseudovariedade dada por

$$[\![\Sigma]\!]_{\mathbf{V}} = \{S \in \mathbf{V} : S \models \Sigma\}.$$

Observação 3.10 *Quando nos referimos a uma pseudoidentidade sem indicar sobre qual pseudovariedade, é porque a estamos a considerar sobre a pseudovariedade* $\mathbf{S}$ *de todos os semigrupos finitos.*

Algumas das pseudovariedades referidas anteriormente podem agora ser apresentadas de forma mais simples. Por exemplo, $\mathbf{G}$ e $\mathbf{N}$ podem ser definidas por pseudoidentidades da seguinte forma:

$$\begin{aligned}
\mathbf{G} &= [\![a^\omega b = ba^\omega = b]\!] \\
\mathbf{N} &= [\![a^\omega b = ba^\omega = a^\omega]\!].
\end{aligned}$$

Note-se que as pseudoidentidades usadas envolvem apenas elementos do subsemigrupo $\Omega_A^\omega \mathbf{S}$. Outros exemplos de pseudovariedades que podem ser descritas desta forma:

$$\begin{aligned}
\mathbf{LI} &= [\![a^\omega b a^\omega = a^\omega]\!] \\
\mathbf{K} &= [\![a^\omega b = a^\omega]\!] \\
\mathbf{D} &= [\![ba^\omega = a^\omega]\!] \\
\mathbf{R} &= [\![(ab)^\omega = (ab)^\omega a]\!] \\
\mathbf{L} &= [\![(ab)^\omega = b(ab)^\omega]\!] \\
\mathbf{J} &= [\![(ab)^\omega a = (ab)^\omega = b(ab)^\omega]\!] \\
&= [\![(ab)^\omega = (ba)^\omega, a^\omega = a^{\omega+1}]\!] \\
\mathbf{A} &= [\![a^\omega = a^{\omega+1}]\!].
\end{aligned}$$

Enunciamos de seguida um resultado que é o análogo para pseudovariedades ao teorema de Birkhoff para variedades.

Teorema 3.11 (Reiterman[29]) *Seja* $\mathcal{W}$ *uma subclasse de uma pseudovariedade* $\mathbf{V}$. *Então,* $\mathcal{W}$ *é uma pseudovariedade se e só se existe um conjunto* Σ *de pseudoidentidades sobre* $\mathbf{V}$ *tal que* $\mathcal{W} = [\![\Sigma]\!]_{\mathbf{V}}$.

Capítulo 4

O problema da ω-palavra

Chegamos enfim, ao tema a que nos propusemos dedicar este trabalho: o estudo do problema da ω-palavra. Uma *assinatura implícita* é um conjunto de operações implícitas contendo a multiplicação. A assinatura $\kappa = \{a \cdot b, a^\omega\}$ é habitualmente designada a *assinatura canónica* sendo a mais usada na teoria de semigrupos finitos quando se trabalha com pseudovariedades aperiódicas, o que é o caso neste trabalho.

Para uma pseudovariedade $\mathbf{V}$, o κ-subsemigrupo de $\overline{\Omega}_A\mathbf{V}$ gerado por A denota-se por $\Omega_A^\kappa\mathbf{V}$. Tendo em consideração as definições introduzidas anteriormente $\Omega_A^\kappa\mathbf{V}$ coincide com o subsemigrupo $\Omega_A^\omega\mathbf{V}$ de $\overline{\Omega}_A\mathbf{V}$. No resto deste trabalho adoptaremos preferencialmente a notação $\Omega_A^\omega\mathbf{V}$ para este subsemigrupo de $\overline{\Omega}_A\mathbf{V}$.

Denotaremos por $p_\mathbf{V} : \Omega_A^\omega\mathbf{S} \to \Omega_A^\omega\mathbf{V}$ o morfismo de ω-semigrupos determinado pela escolha dos geradores. Ou seja, $p_\mathbf{V}$ é a restrição a $\Omega_A^\omega\mathbf{S}$ da projecção natural $q_\mathbf{V} : \overline{\Omega}_A\mathbf{S} \to \overline{\Omega}_A\mathbf{V}$. O problema da ω-palavra para $\mathbf{V}$ é o problema de decidir, para quaisquer ω-palavras π e ρ de $\Omega_A^\omega\mathbf{S}$, se $\mathbf{V}$ satisfaz a pseudoidentidade $\pi = \rho$, ou seja, se $p_\mathbf{V}(\pi) = p_\mathbf{V}(\rho)$.

4.1 Primeiros exemplos

Nesta secção apresentaremos alguns exemplos simples de semigrupos da forma $\overline{\Omega}_A\mathbf{V}$. Em particular, estudaremos o problema da ω-palavra para as pseudovariedades $\mathbf{Sl}, \mathbf{N}, \mathbf{K}$, $\mathbf{D}$ e $\mathbf{LI}$.

Fixemos um alfabeto com n elementos, $A = \{a_1, \ldots, a_n\}$. Os exemplos mais simples de semigrupos da forma $\overline{\Omega}_A\mathbf{V}$ são aqueles em que a pseudovariedade $\mathbf{V}$ é gerada por um conjunto finito de semigrupos, como refere o resultado seguinte [15].

Proposição 4.1 *Seja* $\mathbf{V}$ *uma pseudovariedade de semigrupos. Então as seguintes condições são equivalentes:*

1. $\mathbf{V}$ *é gerada por um conjunto finito de semigrupos;*

2. $\overline{\Omega}_A\mathbf{V} = \Omega_A\mathbf{V}$*;*

3. $\Omega_A\mathbf{V}$ *é finito.*

4.1.1 A Pseudovariedade Sl

Vamos então abordar o problema da ω-palavra, inicialmente sobre a pseudovariedade dos semi-reticulados,

$$\mathbf{Sl} = [\![ab = ba; a^2 = a]\!] \ .$$

Note-se que a pseudovariedade $\mathbf{Sl}$ é um dos casos onde a operação implícita a^ω é explícita. De facto,

$$\forall S \in \mathbf{Sl}\ \forall s \in S \quad (a^\omega)_S(s) = s^\omega = s,$$

o que mostra que a^ω é a operação explícita a sobre $\mathbf{Sl}$.

Como a pseudovariedade $\mathbf{Sl}$ é gerada pelo semi-reticulado $U_1 = \{0, 1\}$ [27], em que 0 é um zero e 1 é a identidade , ela é, em particular, gerada por um conjunto finito de semigrupos. Portanto, pela proposição anterior, $\overline{\Omega}_A\mathbf{Sl} = \Omega_A\mathbf{Sl}$ e $\Omega_A\mathbf{Sl}$ é finito.

O seguinte resultado permite-nos decidir acerca da igualdade de duas quaisquer operações implícitas sobre $\mathbf{Sl}$. Em particular é válido para os elementos de $\Omega_A^\omega\mathbf{S}$ e consequentemente fornece a solução do problema da ω-palavra sobre a pseudovariedade $\mathbf{Sl}$.

Proposição 4.2 *Sejam* $\pi, \rho \in \overline{\Omega}_A\mathbf{S}$. *Então* $\mathbf{Sl} \models \pi = \rho$ *se e só se* $c(\pi) = c(\rho)$.

Demonstração: Note-se que,

$$\mathbf{Sl} \models \pi = \rho \Leftrightarrow \forall S \in \mathbf{Sl},\ S \models \pi = \rho.$$

Comecemos por provar a implicação da esquerda para a direita. Suponhamos que existe $a_r \in A$ tal que a_r pertence ao conteúdo de π mas não pertence ao conteúdo de ρ.

Consideremos o semigrupo U_1 de $\mathbf{Sl}$. Considerando $s_1 = \ldots = s_{r-1} = 1$, $s_r = 0$, $s_{r+1} = \ldots = s_n = 1$, verifica-se que

$$\pi_{U_1}(s_1, \ldots, s_n) = 0 \quad \text{e} \quad \rho_{U_1}(s_1, \ldots, s_n) = 1,$$

portanto, $\pi_{U_1} \neq \rho_{U_1}$, ou seja, $\mathbf{Sl} \not\models \pi = \rho$.

Para provar a implicação contrária suponhamos agora que π e ρ têm o mesmo conteúdo. Usando a identidade $ab = ba$ e o facto de π e ρ coincidirem com operações explícitas sobre $\mathbf{Sl}$ obtém-se que

$$\mathbf{Sl} \models \pi = a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} \quad \text{e} \quad \mathbf{Sl} \models \rho = a_1^{j_1} a_2^{j_2} \cdots a_n^{j_n}$$

para alguns $i_p, j_p \in \mathbb{N}_0$ tais que $i_p = 0$ se e só se $j_p = 0$.

Finalmente, através da identidade $a^2 = a$ deduz-se

$$\mathbf{Sl} \models \pi = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} = \rho, \text{ onde } k_r \in \{0, 1\},$$

ou seja, $\mathbf{Sl} \models \pi = \rho$. □

Note-se que a proposição anterior prova que o semigrupo $\overline{\Omega}_A\mathbf{Sl}$ é isomorfo ao semigrupo $\mathcal{P}(A)$ das partes de A com a operação de união, e munido da topologia discreta. No resto do trabalho identificaremos o semigrupo $\overline{\Omega}_A\mathbf{Sl}$ com o semigrupo $\mathcal{P}(A)$.

Através do resultado que se segue, verifica-se que a função de conteúdo é particularmente bem comportada para toda a pseudovariedade contendo $\mathbf{Sl}$.

Proposição 4.3 (Azevedo [17]) *Seja* $\mathbf{V}$ *uma pseudovariedade contendo* $\mathbf{Sl}$. *Então, a função*

$$c : \overline{\Omega}_A\mathbf{V} \longrightarrow \overline{\Omega}_A\mathbf{Sl}$$

é o único homomorfismo contínuo, tal que $c(a_i) = \{a_i\}$, $i = 1, \ldots, n$. *Ou seja,* c *é a projecção canónica de* $\overline{\Omega}_A\mathbf{V}$ *sobre* $\overline{\Omega}_A\mathbf{Sl}$.

Por exemplo, para uma pseudovariedade $\mathbf{V}$ tal que $\mathbf{Sl} \subseteq \mathbf{V}$, se $a, b, c, d \in A$ então a operação implícita $(ac)^\omega d(b^{\omega+1}cd^\omega)^\omega$ tem conteúdo $\{a, b, c, d\}$.

De seguida, consideremos alguns exemplos de ω-palavras e verifiquemos se a pseudovariedade $\mathbf{Sl}$ satisfaz as igualdades entre elas.

Exemplo 4.4 *Seja $A = \{a, b, c\}$ e sejam $\pi, \rho, \beta, \delta, \tau \in \Omega_A^\omega \mathbf{S}$ tais que:*

- $\pi = b(a(baa)^\omega ac)^\omega ac^\omega bc(ab)^\omega a$;
- $\rho = (ab(a^\omega b)^\omega cab^{\omega+1}c)^\omega abc^\omega c(ac)^\omega ba$;
- $\beta = (aba(a^\omega b)^\omega ab^{\omega+1})^\omega a(abab)^\omega a$;
- $\delta = aba^2c^2$;
- $\tau = bca^2b^3ca$.

Repare-se que as operações implícitas π, ρ, δ e τ têm todas o mesmo conteúdo $\{a, b, c\}$, enquanto que o conteúdo da operação implícita β é o conjunto $\{a, b\}$. Portanto, pela Proposição 4.2, as ω-palavras π, ρ, δ e τ representam sobre $\mathbf{Sl}$ a mesma palavra, e são diferentes de β.

A projecção de uma operação implícita de $\Omega_A^\omega \mathbf{S}$ sobre o semigrupo $\Omega_A^\omega \mathbf{Sl}$ coincide com a restrição da função de conteúdo a $\Omega_A^\omega \mathbf{V}$ (basta considerarmos, na Proposição 4.3, $\mathbf{V}$ como sendo a pseudovariedade $\mathbf{S}$). Assim tem-se,

- $p_{\mathbf{Sl}}(\pi) = \{a, b, c\}$;
- $p_{\mathbf{Sl}}(\rho) = \{a, b, c\}$;
- $p_{\mathbf{Sl}}(\beta) = \{a, b\}$;
- $p_{\mathbf{Sl}}(\delta) = \{a, b, c\}$;
- $p_{\mathbf{Sl}}(\tau) = \{a, b, c\}$.

Dos exemplos considerados, a pseudovariedade $\mathbf{Sl}$ apenas não satisfaz as igualdades entre β e qualquer uma das restantes operações implícitas.

4.1.2 A Pseudovariedade N

Consideremos agora a pseudovariedade dos semigrupos nilpotentes, $\mathbf{N} = [\![a^\omega = 0]\!]$. Comecemos por mostrar que

$$\mathbf{N} = \bigcup_{r\geq 1} [\![a_1 \cdots a_r = 0]\!] \ .$$

Consideremos

$$\mathbf{N}_r = [\![a_1 \cdots a_r = 0]\!] \ .$$

Pretende-se mostrar que $\mathbf{N} = \bigcup_{r\in\mathbb{N}} \mathbf{N}_r$.

Comecemos por mostrar que $\mathbf{N}_r \subseteq \mathbf{N}$, para todo o $r \geq 1$.

Seja $r \in \mathbb{N}$. Como $\mathbf{N}_r \models a_1 \cdots a_r = 0$, em particular, substituindo cada a_i, $i \in \{1, \ldots, r\}$, por a^ω resulta que $\mathbf{N}_r \models a^\omega \cdots a^\omega = 0$. Uma vez que a^ω é idempotente, deduz-se que $\mathbf{N}_r \models a^\omega = 0$. Portanto $\mathbf{N}_r \subseteq \mathbf{N}$ para todo o r, o que prova a inclusão da direita para a esquerda.

Para provar a inclusão contrária mostremos que para todo o $S \in \mathbf{N}$, S satisfaz a igualdade $a_1 \cdots a_r = 0$ para algum $r \in \mathbb{N}$. Sejam $S \in \mathbf{N}$ e $s_1, \ldots, s_r \in S$, com $r \geq |S|$. Pela Proposição 1.11

$$S^r = SE(S)S,$$

e portanto, existem $x, z \in S$ e $y = y^\omega \in E(S)$ tais que

$$s_1 \cdots s_r = xy^\omega z.$$

Dado que $S \in \mathbf{N}$ e $\mathbf{N} \models a^\omega = 0$, também, $S \models a^\omega = 0$. Consequentemente, em S tem-se que $s_1 \cdots s_r = x \cdot 0 \cdot z = 0$. Portanto para todo o $S \in \mathbf{N}$, $S \models a_1 \cdots a_r = 0$, donde $S \in \mathbf{N}_r$.

Conclui-se assim que $\mathbf{N} = \bigcup_{r\in\mathbb{N}} \mathbf{N}_r$.

Para cada $r \in \mathbb{N}$, seja $I_r = A^{\geq r}$ o ideal de A^+ constituído por todas as palavras de comprimento superior ou igual a r. Consideremos ainda o quociente de Rees A^+/I_r. Por definição de A^+/I_r os elementos do ideal I_r são identificados com um só ponto (o qual é um zero). Verifica-se portanto que o conjunto S_r, constituído por todas as palavras sobre A de comprimento inferior a r e por um zero,

$$S_r = \{u \in A^+ : \ |u| < r\} \cup \{0\},$$

munido do produto definido para todos os $u, v \in S_r \backslash \{0\}$ por

$$u \cdot v \ = \ \begin{cases} uv & \text{se } |uv| < r \\ 0 & \text{caso contrário} \end{cases}$$

e

$$u \cdot 0 = 0 = 0 \cdot u = 0 \cdot 0$$

é um semigrupo isomorfo ao quociente de Rees referido.

Em particular o semigrupo S_r pertence a $\mathbf{N}$, pois $S_r \models a_1 \cdots a_r = 0$. Verifiquemos que qualquer identidade válida em S_r é consequência desta.

Suponhamos que $u = v$ é uma identidade sobre $\mathbf{S}$ tal que $S_r \models u = v$.

1) Se $|u| < r$, então em S_r, u é uma palavra finita. Portanto, o comprimento de v também é inferior a r (caso contrário, como $S_r \models a_1 \cdots a_r = 0$, v seria identificada em S_r com o elemento 0 e consequentemente, teriamos que $S_r \not\models u = v$). Para além disso $u = v$, ou seja, u e v são a mesma palavra.

2) Se $|u| \geq r$, então também $|v| \geq r$. Assim para $u = a_1 \cdots a_s$ e $v = b_1 \cdots b_t$, com $s, t \geq r$, tem-se

$$S_r \models \underline{a_1 \cdots a_r}\, .a_{r+1} \cdots a_s = 0.a_{r+1} \cdots a_s = 0 = 0.b_{r+1} \cdots b_t = \underline{b_1 \cdots b_r}\, .b_{r+1} \cdots b_t.$$

De facto, a identidade $u = v$ em S_r é obtida à custa da identidade $a_1 \cdots a_r = 0$.

Deduz-se portanto que $S_r \simeq \Omega_A [\![a_1 \cdots a_r = 0]\!]$. Os semigrupos S_r $(r \geq 1)$ formam um conjunto gerador da pseudovariedade $\mathbf{N}$ nos quais podemos testar a validade de possíveis propriedades de $\mathbf{N}$. Neste contexto, estes semigrupos são designados como *semigrupos-teste*. Mostra-se através deles a proposição seguinte.

Proposição 4.5 *A pseudovariedade* $\mathbf{N}$ *só satisfaz identidades triviais.*

Demonstração: Suponhamos que $u = v$ é uma identidade tal que $\mathbf{N} \models u = v$. Note-se que

$$\mathbf{N} \models u = v \ \Leftrightarrow \ \forall r \in \mathbb{N}, \ S_r \models u = v,$$

pois os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{N}$. Consideremos $r = |u| + 1$. Então, como $S_r \models u = v$, deduz-se que $u = v$. $\square$

Conclui-se da proposição anterior que $\Omega_A\mathbf{N} \simeq A^+$, ou seja, cada operação explícita sobre $\mathbf{N}$ escreve-se de forma única à custa dos elementos $\{a_1, \ldots, a_n\}$. Mais geralmente, tem-se o seguinte corolário, que caracteriza as operações explícitas sobre uma pseudovariedade $\mathbf{V}$, caso $\mathbf{V}$ contenha a pseudovariedade $\mathbf{N}$.

Corolário 4.6 *Se* $\mathbf{V}$ *é uma pseudovariedade de semigrupos tal que* $\mathbf{N} \subseteq \mathbf{V}$*, então* $\Omega_A\mathbf{V} = A^+$.

Seja $(w_n)_n$ uma sucessão em $\Omega_A\mathbf{N}$ e suponhamos que $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{N}$, digamos para $\pi \in \overline{\Omega}_A\mathbf{N}$. Ora

$$\begin{aligned}\lim_{n\to+\infty} w_n = \pi \quad &\Leftrightarrow \quad \lim_{n\to+\infty}(w_n)_S = \pi_S, \quad \forall S \in \mathbf{N},\\ &\Leftrightarrow \quad \lim_{n\to+\infty}(w_n)_{S_r} = \pi_{S_r}, \quad \forall r \in \mathbb{N},\end{aligned}$$

pois como já referimos, os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{N}$. Temos então uma das seguintes situações:

1) $|w_n| \nrightarrow \infty$, ou seja, existe um $p \in \mathbb{N}$ tal que para todo o n, $|w_n| \leq p$. Dado que, para $r > p$, $(w_n)_n$ converge em S_r, deduz-se que w_n é ultimamente constante (isto é, é constante a partir de uma certa ordem), digamos igual a u.

   Conclui-se então que $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{N}$ para $u \in A^+$.

2) $|w_n| \to \infty$, ou seja, para todo o $r \in \mathbb{N}$, $|w_n| \geq r$ a partir de uma certa ordem, que depende de r. Então, $w_n = 0$ em S_r a partir dessa ordem, o que mostra que $(w_n)_n$ converge para 0 em cada S_r. Conclui-se assim que π é um zero de $\overline{\Omega}_A\mathbf{N}$, que denotamos por 0 como habitualmente.

Portanto, $\overline{\Omega}_A\mathbf{N} = \Omega_A\mathbf{N} \cup \{0\}$, ou seja, $\overline{\Omega}_A\mathbf{N}$ é obtido de $\Omega_A\mathbf{N}$ acrescentando um “ponto no infinito”o qual é um zero. O produto em $\overline{\Omega}_A\mathbf{N}$ é dado para todos os $u, v \in A^+$ por

$$\begin{aligned}u \cdot v \quad &= \quad uv;\\ u \cdot 0 = 0 \quad &= \quad 0 \cdot u = 0 \cdot 0.\end{aligned}$$

No exemplo que se segue trata-se o problema da ω-palavra sobre a pseudovariedade $\mathbf{N}$. As operações implícitas mencionadas no Exemplo 4.4 continuam a ser as utilizadas. O objectivo é realçar que há alterações na satisfação de pseudoidentidades com a passagem de uma pseudovariedade para outra.

Exemplo 4.7 *Consideremos então as operações implícitas $\pi, \rho, \beta, \delta, \tau \in \Omega_A^\omega \mathbf{S}$ do Exemplo 4.4.*

- $\pi = b(a(baa)^\omega ac)^\omega ac^\omega bc(ab)^\omega a$;
- $\rho = (ab(a^\omega b)^\omega cab^{\omega+1}c)^\omega abc^\omega c(ac)^\omega ba$;
- $\beta = (aba(a^\omega b)^\omega ab^{\omega+1})^\omega a(abab)^\omega a$;
- $\delta = aba^2c^2$;
- $\tau = bca^2b^3ca$.

A projecção de cada uma das operações implícitas sobre o semigrupo $\Omega_A^\omega \mathbf{N}$ é a seguinte:

- $p_{\mathbf{N}}(\pi) = 0$;
- $p_{\mathbf{N}}(\rho) = 0$;
- $p_{\mathbf{N}}(\beta) = 0$;
- $p_{\mathbf{N}}(\delta) = aba^2c^2$;
- $p_{\mathbf{N}}(\tau) = bca^2b^3ca$.

Dado que as ω-palavras π, ρ e β são operações não explícitas, são identificadas sobre $\mathbf{N}$ com o elemento 0. Portanto, $\mathbf{N} \models \pi = \rho = \beta$. As ω-palavras δ e τ são explícitas, ou seja, δ e τ estão em A^+. Como não são a mesma palavra de A^+, então são distintas sobre a pseudovariedade $\mathbf{N}$. Portanto, $\mathbf{N} \not\models \delta = \tau$. Note-se ainda que, dadas duas ω-palavras γ e η de $\overline{\Omega}_A\mathbf{S}$, se γ é explícita e η não, então na pseudovariedade $\mathbf{N}$ a igualdade entre γ e η nunca é satisfeita.

4.1.3 A Pseudovariedade K

Consideremos a pseudovariedade $\mathbf{K}$ dos semigrupos nos quais os idempotentes são zeros à esquerda, $\mathbf{K} = [\![a^\omega b = a^\omega]\!]$. Verifiquemos que podemos escrevê-la como

$$\mathbf{K} = \bigcup_{r\geq 1} [\![a_1 \cdots a_r b = a_1 \cdots a_r]\!] \ .$$

Consideremos
$$\mathbf{K}_r = [\![a_1 \cdots a_r b = a_1 \cdots a_r]\!] \ .$$
Pretende-se mostrar que $\mathbf{K} = \bigcup_{r\in\mathbb{N}} \mathbf{K}_r$.

Comecemos por mostrar que $\mathbf{K}_r \subseteq \mathbf{K}$, para todo o $r \geq 1$.

Seja $r \in \mathbb{N}$. Como $\mathbf{K}_r \models a_1 \cdots a_r b = a_1 \cdots a_r$, em particular, substituindo cada a_i, $i \in \{1, \ldots, r\}$ por a^ω, tem-se que $\mathbf{K}_r \models a^\omega \cdots a^\omega b = a^\omega \cdots a^\omega$. Como a^ω é idempotente, conclui-se que $\mathbf{K}_r \models a^\omega b = a^\omega$. Portanto $\mathbf{K}_r \subseteq \mathbf{K}$ para todo o r, o que prova a inclusão da direita para a esquerda.

Para provar a inclusão contrária pretende-se mostrar que para todo o S pertencente a $\mathbf{K}$, S satisfaz a identidade $a_1 \cdots a_r b = a_1 \cdots a_r$, para algum $r \in \mathbb{N}$. Sejam $S \in \mathbf{K}$ e $s_1, \ldots, s_r, t \in S$, com $r \geq |S|$. Pela Proposição 1.11, existem $x, z \in S$ e $y = y^\omega \in E(S)$ tais que
$$s_1 \cdots s_r = xy^\omega z$$
donde
$$s_1 \cdots s_r t = xy^\omega zt.$$
Uma vez que y^ω é idempotente de S e $S \in \mathbf{K}$, então y^ω é um zero à esquerda. Consequentemente verifica-se em S, $xy^\omega z = xy^\omega = xy^\omega zt$. Portanto $s_1 \cdots s_r t = s_1 \cdots s_r$. Tem-se então, para todo o $S \in \mathbf{K}$, que $S \models a_1 \cdots a_r b = a_1 \cdots a_r$.

Conclui-se assim que $\mathbf{K} = \bigcup_{r\in\mathbb{N}} \mathbf{K}_r$.

Como $\mathbf{N} \subseteq \mathbf{K}$, deduz-se do Corolário 4.6 que $\Omega_A \mathbf{K} = A^+$.

Para cada inteiro $r \in \mathbb{N}$, consideremos o semigrupo
$$\Omega_A [\![a_1 \cdots a_r b = a_1 \cdots a_r]\!] \ .$$
De forma análoga ao caso de $\mathbf{N}$, prova-se que este semigrupo é isomorfo ao semigrupo S_r cujo conjunto suporte é formado por todas as palavras sobre A de comprimento inferior ou igual a r, e onde o produto é dado para todos os $u, v \in S_r$ por
$$u \cdot v \ = \ \begin{cases} uv & \text{se } |uv| \leq r \\ p_r(uv) & \text{se } |uv| > r. \end{cases}$$
Os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{K}$.

De seguida, mostra-se que uma sucessão $(w_n)_n$ de A^+ converge em $\overline{\Omega}_A\mathbf{K}$ se e só se é ultimamente constante, ou $|w_n| \to \infty$ e

$$\forall r \in \mathbb{N}\ \exists n_r \in \mathbb{N}, i, j \geq n_r \ \Rightarrow\ w_i \text{ e } w_j \text{ têm o mesmo prefixo de comprimento } r.$$

Seja $(w_n)_n$ uma sucessão de $\Omega_A\mathbf{K}$ e suponhamos que $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{K}$, digamos para $\pi \in \overline{\Omega}_A\mathbf{K}$. Uma vez que os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{K}$, $(w_n)_n$ converge em cada S_r e, portanto, ou $w_n = u$ para algum $u \in A^+$ e para todo o n suficientemente grande, ou $|w_n| \to \infty$ e $p_r(w_n)$ é constante para todo o n suficientemente grande. Conclui-se assim que, ou $\pi = u$ é explícita, ou π não é explícita e é um zero à esquerda em cada S_r e portanto π é um zero à esquerda. Conclui-se ainda no caso de π não ser explícita o seguinte.

Corolário 4.8 *Se $\pi \in \overline{\Omega}_A\mathbf{K}\backslash\Omega_A\mathbf{K}$, então π pode ser identificada com a palavra infinita à direita*

$$a_1a_2a_3\cdots \in A^{\mathbb{N}}$$

em que a_i é a $i-$ésima letra de π, isto é, se $(w_n)_{n\in\mathbb{N}}$ é uma sucessão de operações explícitas a convergir para π, então a_i é a $i-$ésima letra de todos os termos de w_n a partir de uma certa ordem.

Conclui-se assim que $\overline{\Omega}_A\mathbf{K} = A^+ \cup A^{\mathbb{N}}$, ou seja, o semigrupo das operações implícitas sobre $\mathbf{K}$ é formado pelas palavras de A^+ e pelas palavras infinitas à direita sobre A. O produto em $\overline{\Omega}_A\mathbf{K}$ define-se, para todos os $u, v \in A^+$ e todos os $w, z \in A^{\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ u \cdot w &= uw; \\ w \cdot u &= w = w \cdot z. \end{aligned}$$

Tratemos agora, o problema da ω-palavra sobre a pseudovariedade $\mathbf{K}$ consideradas as operações implícitas $\pi, \rho, \beta, \delta, \tau \in \Omega_A^\omega\mathbf{S}$ já referidas nos Exemplos 4.4 e 4.7:

- $\pi = b(a(baa)^\omega ac)^\omega ac^\omega bc(ab)^\omega a$;
- $\rho = (ab(a^\omega b)^\omega cab^{\omega+1}c)^\omega abc^\omega c(ac)^\omega ba$;
- $\beta = (aba(a^\omega b)^\omega ab^{\omega+1})^\omega a(abab)^\omega a$;

- $\delta = aba^2c^2$;
- $\tau = bca^2b^3ca$.

A projecção de cada uma das operações implícitas sobre o semigrupo $\Omega_A^\omega \mathbf{K}$ é dada, respectivamente, por

- $p_{\mathbf{K}}(\pi) = b(aba)^{+\infty}$;
- $p_{\mathbf{K}}(\rho) = aba^{+\infty}$;
- $p_{\mathbf{K}}(\beta) = aba^{+\infty}$;
- $p_{\mathbf{K}}(\delta) = aba^2c^2$;
- $p_{\mathbf{K}}(\tau) = bca^2b^3ca$.

Como se ilustra neste exemplo, o semigrupo $\Omega_A^\omega \mathbf{K}$ é formado pelas palavras finitas e pelas palavras infinitas à direita ultimamente periódicas. Neste exemplo as palavras infinitas são já apresentadas na sua forma canónica. Assim verifica-se que as ω-palavras ρ e β representam sobre $\mathbf{K}$ a mesma palavra. Quanto à ω-palavra π, $\mathbf{K} \not\models \pi = \rho$, pois $b(aba)^{+\infty}$ e $aba^{+\infty}$ são palavras infinitas à direita distintas. As ω-palavras δ e τ são explícitas e como não representam a mesma palavra finita são distintas sobre $\mathbf{K}$. Portanto, $\mathbf{K} \not\models \delta = \tau$.

4.1.4 A Pseudovariedade D

Uma vez que $\mathbf{D}$ é a pseudovariedade dos semigrupos nos quais os idempotentes são zeros à direita, o estudo das operações implícitas sobre $\mathbf{D}$ realiza-se de forma análoga ao anterior. Assim, para a pseudovariedade $\mathbf{D} = [\![ba^\omega = a^\omega]\!]$, verifica-se:

- $\mathbf{D} = \bigcup_{r \geq 1} [\![ba_1 \cdots a_r = a_1 \cdots a_r]\!]$;
- $\Omega_A \mathbf{D} = A^+$;
- $\overline{\Omega}_A \mathbf{D} = A^+ \cup A^{-\mathbb{N}}$, ou seja, os elementos não explícitos de $\overline{\Omega}_A \mathbf{D}$ são identificados com palavras infinitas à esquerda de $A^{-\mathbb{N}}$;

- O produto em $\overline{\Omega}_A\mathbf{D}$ define-se, para todos os $u, v \in A^+$ e todos os $w, z \in A^{-\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ w \cdot u &= wu; \\ u \cdot w &= w = z \cdot w. \end{aligned}$$

Passemos, então, ao estudo do exemplo onde é tratado o problema da ω--palavra, agora sobre a pseudovariedade $\mathbf{D}$. Tendo em consideração as ω-palavras $\pi, \rho, \beta, \delta,\ \tau \in \Omega_A^\omega\mathbf{S}$ anteriormente apresentadas, segue que a projecção de cada uma delas sobre o semigrupo $\Omega_A^\omega\mathbf{D}$ é dada respectivamente por

- $p_{\mathbf{D}}(\pi) = (ba)^{-\infty}$;
- $p_{\mathbf{D}}(\rho) = (ac)^{-\infty}ba$;
- $p_{\mathbf{D}}(\beta) = (ba)^{-\infty}$;
- $p_{\mathbf{D}}(\delta) = aba^2c^2$;
- $p_{\mathbf{D}}(\tau) = bca^2b^3ca$.

Analogamente ao que foi apresentado anteriormente para $\mathbf{K}$ ilustra-se neste exemplo que o semigrupo $\Omega_A^\omega\mathbf{D}$ é formado pelas palavras finitas e pelas palavras infinitas à esquerda ultimamente periódicas. Também neste exemplo as palavras infinitas são já apresentadas na sua forma canónica. Assim verifica-se que as ω-palavras π e β representam sobre $\mathbf{D}$ a mesma palavra. Quanto às formas canónicas $(ba)^{-\infty}$ e $(ac)^{-\infty}ba$, respectivamente das projecções de π e de ρ sobre $\mathbf{D}$, são palavras infinitas à esquerda distintas. Portanto $\mathbf{D} \not\models \pi = \rho$. Para as ω-palavras δ e τ o tratamento é análogo ao realizado para a pseudovariedade $\mathbf{K}$. Portanto, $\mathbf{D} \not\models \delta = \tau$.

4.1.5 A Pseudovariedade LI

Tratemos agora o caso da pseudovariedade $\mathbf{LI} = [\![a^\omega ba^\omega = a^\omega]\!]$ dos semigrupos localmente triviais, também dada por

$$\mathbf{LI} = \bigcup_{r \geq 1} [\![a_1 \cdots a_r b c_1 \cdots c_r = a_1 \cdots a_r c_1 \cdots c_r]\!] \ .$$

Como $\mathbf{N} \subseteq \mathbf{LI}$, deduz-se do Corolário 4.6 que $\Omega_A\mathbf{LI} = A^+$.

Prova-se que uma sucessão $(w_n)_n$ de $\Omega_A\mathbf{LI}$ converge em $\overline{\Omega}_A\mathbf{LI}$ se e só se é ultimamente constante, ou $|w_n| \to \infty$ e

$$\forall r \in \mathbb{N}\ \exists t_r \in \mathbb{N}, i, j \geq t_r \Rightarrow \begin{array}{c} w_i \text{ e } w_j \text{ têm o mesmo prefixo e} \\ \text{o mesmo sufixo de comprimento } r. \end{array}$$

Então, as operações implícitas não explícitas sobre $\mathbf{LI}$ podem ser identificadas com o conjunto $\{(w, w') : \ w \in A^{\mathbb{N}}, w' \in A^{-\mathbb{N}}\}$, ou seja, $\overline{\Omega}_A\mathbf{LI} = A^+ \cup (A^{\mathbb{N}} \times A^{-\mathbb{N}})$. O produto em $\overline{\Omega}_A\mathbf{LI}$ é dado, para todos os $u, v \in A^+$ e todos os $(w, z), (w', z') \in A^{\mathbb{N}} \times A^{-\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ u \cdot (w, z) &= (uw, z); \\ (w, z) \cdot u &= (w, zu); \\ (w, z) \cdot (w', z') &= (w, z'). \end{aligned}$$

Note-se que $\mathbf{K} \cap \mathbf{D} = \mathbf{N}$ e $\mathbf{K} \vee \mathbf{D} = \mathbf{LI}$. A segunda igualdade é uma consequência imediata do estudo das operações implícitas sobre $\mathbf{K}$, $\mathbf{D}$ e $\mathbf{LI}$ e do resultado seguinte, que é uma consequência imediata do teorema de Reiterman.

Proposição 4.9 *Sejam* $\mathbf{V}$ *e* $\mathbf{W}$ *duas pseudovariedades e sejam* $\pi, \rho \in \overline{\Omega}_A\mathbf{S}$ *duas operações implícitas. Então*

$$\mathbf{V} \vee \mathbf{W} \models \pi = \rho \quad \textit{se e só se} \quad \mathbf{V}, \mathbf{W} \models \pi = \rho.$$

Demonstração: Se $\mathbf{V} \vee \mathbf{W}$ satisfaz a pseudoidentidade $\pi = \rho$, então é imediato que $\mathbf{V}$ e $\mathbf{W}$ também a satisfazem.

Reciprocamente, suponhamos que $\mathbf{V}$ e $\mathbf{W}$ satisfazem a pseudoidentidade $\pi = \rho$ mas $\mathbf{V} \vee \mathbf{W}$ não a satisfaz. Seja Σ uma base de pseudoidentidades de $\mathbf{V} \vee \mathbf{W}$, ou seja, $\mathbf{V} \vee \mathbf{W} = [\![\Sigma]\!]$. Existe portanto, uma pseudovariedade $\mathbf{U}$ tal que

$$\mathbf{U} = [\![\Sigma \cup \{\pi = \rho\}]\!] \subsetneq \mathbf{V} \vee \mathbf{W}$$

mas dado que $\mathbf{V}$ e $\mathbf{W}$ estão contidas em $\mathbf{U}$, isto é absurdo por definição de supremo, pois o supremo de $\mathbf{V}$ e $\mathbf{W}$ é a menor pseudovariedade que contém ambas. □

Portanto o estudo do problema da ω-palavra sobre $\mathbf{LI}$ está interligado ao estudo sobre $\mathbf{K}$ e $\mathbf{D}$.

Consideremos, uma vez mais, as ω-palavras π, ρ, β, δ e τ de $\Omega_A^\omega\mathbf{S}$. Tendo em conta os estudos já efectuados para as pseudovariedades $\mathbf{K}$ e $\mathbf{D}$ podemos concluir, por aplicação directa da proposição anterior, que dadas quaisquer duas ω-palavras de entre as apresentadas, a pseudovariedade $\mathbf{LI}$ não satisfaz a igualdade entre elas. De facto, observando quais as igualdades satisfeitas pela pseudovariedade $\mathbf{K}$ e quais as igualdades satisfeitas pela pseudovariedade $\mathbf{D}$ é imediato concluir que nenhuma é comum. Por exemplo, $\mathbf{K}$ satisfaz a igualdade entre ρ e β mas $\mathbf{D}$ não satisfaz, e consequentemente, $\mathbf{LI}$ também não a satisfaz.

Para finalizar, apresentemos um exemplo de dois elementos de $\Omega_A^\omega\mathbf{S}$ (onde $A = \{a, b, c, d\}$) para as quais a igualdade sobre $\mathbf{LI}$ é satisfeita.

Exemplo 4.10 *Sejam $\pi, \rho \in \Omega_A^\omega\mathbf{S}$ as seguintes ω-palavras:*

- $\pi = ((ab^\omega)^\omega cab^{\omega+1}c)^\omega bc^\omega c(ac)^\omega ba$;
- $\rho = abb^\omega c(ad^\omega)^{\omega+1}(ca)^\omega cba$.

A projecção de uma ω-palavra não explícita sobre o semigrupo $\Omega_A^\omega\mathbf{LI}$ é o par constituído pelas projecções dessa mesma operação sobre os semigrupos $\Omega_A^\omega\mathbf{K}$ e $\Omega_A^\omega\mathbf{D}$, respectivamente. Portanto,

- $p_{\mathbf{LI}}(\pi) = (ab^{+\infty}, (ac)^{-\infty}ba)$;
- $p_{\mathbf{LI}}(\rho) = (ab^{+\infty}, (ac)^{-\infty}ba)$.

Neste exemplo as palavras infinitas são já apresentadas na sua forma canónica. Assim verifica-se que $\mathbf{K} \models \pi = \rho$ e também $\mathbf{D} \models \pi = \rho$. Conclui-se então que $p_{\mathbf{LI}}(\pi)$ e $p_{\mathbf{LI}}(\rho)$ coincidem, ou seja, $\mathbf{LI} \models \pi = \rho$.

Capítulo 5

As ω-palavras sobre LSl

Normalmente $\overline{\Omega}_A\mathbf{V}$ não é constituído apenas por ω-palavras, como vimos já no caso das pseudovariedades $\mathbf{K}$, $\mathbf{D}$, e $\mathbf{LI}$. Este é também o caso do semigrupo $\overline{\Omega}_A\mathbf{LSl}$ que está muito longe de ser constituído apenas por ω-palavras. Para mais informação consultar em [21] o capítulo nove.

5.1 A Pseudovariedade LSl

Neste capítulo mostra-se que é possível decidir efectivamente a igualdade entre duas ω-palavras sobre a pseudovariedade $\mathbf{LSl}$ dos semigrupos finitos localmente idempotentes e localmente comutativos, ou seja, dos semigrupos S tais que $eSe \in \mathbf{Sl}$ para todo o $e \in E(S)$.

Comecemos por apresentar uma caracterização das operações implícitas sobre $\mathbf{LSl}$. Verifiquemos primeiro que $\mathbf{LI} \subseteq \mathbf{LSl}$. Note-se que

$$\mathbf{LI} = [\![a^\omega b a^\omega = a^\omega]\!]\ , \quad \mathbf{LSl} = [\![a^\omega b a^\omega b a^\omega = a^\omega b a^\omega,\ a^\omega b a^\omega c a^\omega = a^\omega c a^\omega b a^\omega]\!]\ .$$

Seja $S \in \mathbf{LI}$. Então $S \models a^\omega b a^\omega = a^\omega$ e consequentemente,

$$S \models a^\omega b a^\omega b a^\omega = a^\omega = a^\omega b a^\omega.$$

Verifica-se também que $S \models a^\omega b a^\omega c a^\omega = a^\omega = a^\omega c a^\omega b a^\omega$. Logo $S \in \mathbf{LSl}$.

Uma vez verificada a inclusão $\mathbf{LI} \subseteq \mathbf{LSl}$, o semigrupo livre A^+ pode ser visto como um subsemigrupo de $\overline{\Omega}_A\mathbf{LSl}$ ($\Omega_A\mathbf{LSl} = A^+$).

A notação $Fact(\pi)$ é utilizada para representar o conjunto de todas as palavras $u \in A^+$ tais que u é factor de π, ou seja, tais que $\pi = \rho u \alpha$ com ρ, α pertencentes ao monoíde $(\overline{\Omega}_A\mathbf{LSl})^1$.

Proposição 5.1 (Costa [21]) *Sejam $\pi, \rho \in \overline{\Omega}_A\mathbf{LSl}$. Então, $\pi = \rho$ se e só se $Fact(\pi) = Fact(\rho)$ e $\mathbf{LI} \models \pi = \rho$.*

A proposição seguinte caracteriza as sucessões de A^+ que convergem em $\overline{\Omega}_A\mathbf{LSl}$.

Proposição 5.2 (Costa [21]) *Seja $(v_k)_k$ uma sucessão de A^+. Então a sucessão $(v_k)_k$ converge em $\overline{\Omega}_A\mathbf{LSl}$ se e só se ela converge em $\overline{\Omega}_A\mathbf{LI}$ e toda a palavra finita é factor de um número finito de termos ou de quase todos os termos da sucessão.*

Consideremos uma sucessão $(v_k)_k$ de A^+. Denota-se por $Fact_\infty((v_k)_k)$ o conjunto de todas as palavras de A^+ que são factores de v_k para todo o $k \in \mathbb{N}$ a partir de uma certa ordem, isto é, que são factores de quase todos os termos da sucessão $(v_k)_k$.

Corolário 5.3 *Seja $(v_k)_k$ uma sucessão de A^+ tal que $(v_k)_k$ converge para π em $\overline{\Omega}_A\mathbf{LSl}$. Então, $Fact(\pi) = Fact_\infty((v_k)_k)$.*

Para ω-palavras de um certo tipo é possível descrever os seus factores finitos de uma forma mais explícita.

Lema 5.4 *Seja $\pi \in \overline{\Omega}_A\mathbf{LSl} \backslash A^+$ e suponhamos que π admite uma factorização do tipo $\pi = u_0 x_1^\omega u_1 x_2^\omega \cdots x_k^\omega u_k$ onde $k \in \mathbb{N}$, $u_0, \ldots, u_k \in A^*$ e $x_1, \ldots, x_k \in A^+$. Então*

$$Fact(\pi) = Fact(u_0 x_1^{+\infty}) \cup \left(\bigcup_{i=1}^{k-1} Fact(x_i^{-\infty} u_i x_{i+1}^{+\infty}) \right) \cup Fact(x_k^{-\infty} u_k).$$

Demonstração: Uma vez que em $\overline{\Omega}_A\mathbf{LSl}$ o limite da sucessão $(x_i^m)_m$ é x_i^ω e tendo em conta a continuidade da multiplicação, podemos deduzir sucessivamente

$$\begin{aligned} \pi &= u_0 x_1^\omega u_1 x_2^\omega \cdots x_k^\omega u_k \\ &= \lim_m u_0 \cdot \lim_m x_1^m \cdots \lim_m x_k^m \cdot \lim_m u_k \\ &= \lim_m (u_0 x_1^m \cdots x_k^m u_k). \end{aligned}$$

Assim, tomando $v_m = u_0 x_1^m \cdots x_k^m u_k$, tem-se que a sucessão $(v_m)_m$ converge para π. Portanto, pelo Corolário 5.3, $Fact(\pi) = Fact_\infty((v_m)_m)$. Mas,

$$Fact_\infty((v_m)_m) = Fact(u_0 x_1^{+\infty}) \cup \left(\bigcup_{i=1}^{k-1} Fact(x_i^{-\infty} u_i x_{i+1}^{+\infty}) \right) \cup Fact(x_k^{-\infty} u_k)$$

o que prova o resultado. □

De seguida mostraremos que todas as ω-palavras sobre **LSl** são do tipo descrito no Lema 5.4. Para tal, o seguinte resultado será bastante útil.

Proposição 5.5 (Almeida [4]) *Seja* **V** *uma pseudovariedade e suponhamos que* $\pi \in \overline{\Omega}_A\mathbf{V}$ *é não explícita. Então existem* $\beta, \delta, \rho \in \overline{\Omega}_A\mathbf{V}$ *tais que* $\pi = \beta\delta^\omega\rho$.

O resultado anterior constitui uma generalização da Proposição 1.11 e tem como consequência o resultado seguinte.

Lema 5.6 *Se* $\pi \in \overline{\Omega}_A\mathbf{LSl} \backslash A^+$, *então* $\pi^\omega = \pi^2$.

Demonstração: Pela Proposição 5.5, existem $\beta, \delta, \rho \in \overline{\Omega}_A\mathbf{V}$ tais que $\pi = \beta\delta^\omega\rho$. Portanto

$$\begin{aligned}(\pi^2)^2 &= \pi \cdot \pi \cdot \pi \cdot \pi \\ &= (\beta\delta^\omega\rho)(\beta\delta^\omega\rho)(\beta\delta^\omega\rho)(\beta\delta^\omega\rho),\end{aligned}$$

e como $\overline{\Omega}_A\mathbf{LSl}$ satisfaz a pseudoidentidade $a^\omega b a^\omega b a^\omega = a^\omega b a^\omega$, então

$$\begin{aligned}(\pi^2)^2 &= \beta\delta^\omega(\rho\beta)\delta^\omega(\rho\beta)\delta^\omega(\rho\beta)\delta^\omega\rho \\ &= \beta\delta^\omega(\rho\beta)\delta^\omega\rho \\ &= (\beta\delta^\omega\rho)(\beta\delta^\omega\rho) \\ &= \pi^2.\end{aligned}$$

Concluimos assim que π^2 é idempotente, ou seja, que $\pi^\omega = \pi^2$. □

O resultado seguinte permite-nos garantir a decibilidade da igualdade entre duas ω-palavras sobre a pseudovariedade **LSl**.

Teorema 5.7 *Se* $\pi \in \overline{\Omega}_A\mathbf{LSl}$ *é uma* ω*-palavra, então* π *admite uma factorização*

$$\pi = u_0 x_1^\omega u_1 x_2^\omega \cdots x_k^\omega u_k,$$

com $k \in \mathbb{N}_0$, $u_0, \ldots, u_k \in A^*$, $u_0 \neq 1$ *se* $\pi = u_0$ *e* $x_1, \ldots, x_k \in A^+$.
Para além disso, se $\rho = v_0 y_1^\omega v_1 y_2^\omega \cdots y_l^\omega v_l$ *é uma outra factorização do mesmo*

tipo, então verifica-se a igualdade $\pi = \rho$ se e só se, ou $k = l = 0$ e $u_0 = v_0$, ou $k, l \geq 1$, $u_0x_1^{+\infty} = v_0y_1^{+\infty}$, $x_k^{-\infty}u_k = y_l^{-\infty}v_l$ e são iguais os seguintes conjuntos

$$I_\pi = \{x_i^\infty, x_j^{-\infty}u_jx_{j+1}^{+\infty} | 1 \leq i \leq k, 1 \leq j \leq k-1\}$$

e

$$I_\rho = \{y_i^\infty, y_j^{-\infty}v_jy_{j+1}^{+\infty} | 1 \leq i \leq l, 1 \leq j \leq l-1\}.$$

Em particular, podemos decidir efectivamente se $\pi = \rho$.

Demonstração: Uma vez que π é uma ω-palavra, admite uma factorização da forma

$$\pi = w_0\pi_1^\omega w_1\pi_2^\omega \cdots \pi_m^\omega w_m$$

com $m \in \mathbb{N}_0$, $w_0, \ldots, w_m \in A^*$ e $\pi_1, \ldots, \pi_m \in \Omega_A^\omega\mathbf{LSl}$. Portanto, para $i \in \{1, \ldots, m\}$ ou π_i é explícita e então $\pi_i \in A^+$, ou π_i não é explícita e consequentemente, pelo Lema 5.6, podemos substituir o factor π_i^ω por π_i^2. Como ω aparece na escrita de π um número finito de vezes, então, por aplicação sucessiva da substituição referida anteriormente obtém-se, ao fim de um número finito de passos, uma factorização para π do mesmo tipo que a do enunciado.

Consideremos agora

$$\pi = u_0x_1^\omega u_1x_2^\omega \cdots x_k^\omega u_k$$

e

$$\rho = v_0y_1^\omega v_1y_2^\omega \cdots y_l^\omega v_l,$$

duas factorizações da mesma forma que as referidas no enunciado. Se $k = l = 0$, então $\pi = \rho$ se e só se $u_0 = v_0$. Se $k = 0$ e $l \neq 0$ (ou vice-versa), então não é possível verificar-se $\pi = \rho$ pois teríamos a igualdade entre uma operação explícita e uma não explícita. Tratemos então o caso em que $k, l \geq 1$. Sabe-se, pela Proposição 5.1, que $\pi = \rho$ se e só se $Fact(\pi) = Fact(\rho)$ e $\mathbf{LI} \models \pi = \rho$. Uma vez estudada a pseudovariedade **LI** tem-se que as restrições de π e ρ a **LI** são

$$(u_0x_1^{+\infty}, x_k^{-\infty}u_k) \quad \text{e} \quad (v_0y_1^{+\infty}, y_l^{-\infty}v_l),$$

respectivamente. Por outro lado, sabemos pelo Lema 5.4 que $Fact(\pi)$ é o conjunto

$$F_\pi = Fact(u_0x_1^{+\infty}) \cup \left(\bigcup_{i=1}^{k-1} Fact(x_i^{-\infty}u_ix_{i+1}^{+\infty})\right) \cup Fact(x_k^{-\infty}u_k)$$

e que $Fact(\rho)$ é o conjunto

$$F_\rho = Fact(v_0 y_1^{+\infty}) \cup \left(\bigcup_{i=1}^{l-1} Fact(y_i^{-\infty} v_i y_{i+1}^{+\infty}) \right) \cup Fact(y_l^{-\infty} v_l).$$

Portanto na hipótese de se ter $\pi = \rho$ deduz-se que $u_0 x_1^{+\infty} = v_0 y_1^{+\infty}$, $x_k^{-\infty} u_k = y_l^{-\infty} v_l$ e que $F_\pi = F_\rho$. Mostremos que $F_\pi = F_\rho$ implica a igualdade $I_\pi = I_\rho$. Tomemos para tal $w \in I_\pi$. Então w é uma palavra ultimamente periódica da forma $w = x_i^\infty$ $(1 \leq i \leq k)$, ou da forma $w = x_j^{-\infty} u_j x_{j+1}^{+\infty}$ $(1 \leq j \leq k-1)$. Consideremos o conjunto

$$F'_\rho = \{v_0 y_1^{+\infty}, y_l^{-\infty} v_l\} \cup \{y_i^{-\infty} v_i y_{i+1}^{+\infty} |\ 1 \leq i \leq l-1\}.$$

Como w é de uma das formas referidas anteriormente, então $Fact(w) \subseteq F_\pi$. Mas $F_\pi = F_\rho$, e consequentemente, $Fact(w) \subseteq F_\rho = Fact(F'_\rho)$. Logo, pelo Lema 2.13, como F'_ρ é um conjunto finito de $A^{\mathbb{N}} \cup A^{-\mathbb{N}} \cup A^{\widetilde{\mathbb{Z}}}$ então existe $z \in F'_\rho$ tal que $Fact(w) \subseteq Fact(z)$. Agora, se $z = v_0 y_1^{+\infty}$ ou $z = y_l^{-\infty} v_l$, então, pelo Lema 2.12, como $Fact(w) \subseteq Fact(z)$ tem-se $w = y_1^\infty$ ou $w = y_l^\infty$, respectivamente, concluindo-se assim que $w \in I_\rho$. Se $z = y_i^{-\infty} v_i y_{i+1}^{+\infty}$ para algum $1 \leq i \leq l-1$, como $Fact(w) \subseteq Fact(z)$ tem-se, pelo Lema 2.11, que $w = z$ ou $w = y_i^\infty$ com $1 \leq i \leq l$, e portanto $w \in I_\rho$. Provamos assim a inclusão $I_\pi \subseteq I_\rho$. Por simetria verifica-se que $I_\pi \supseteq I_\rho$, deduzindo-se desta forma a igualdade $I_\pi = I_\rho$.

Reciprocamente suponhamos que $u_0 x_1^{+\infty} = v_0 y_1^{+\infty}$, $x_k^{-\infty} u_k = y_l^{-\infty} v_l$ e $I_\pi = I_\rho$. É imediato que **LI** $\models \pi = \rho$. Pela Proposição 5.1, para concluir a igualdade $\pi = \rho$ resta mostrar que a igualdade $I_\pi = I_\rho$ implica $F_\pi = F_\rho$. Consideremos, então, $w \in A^+$ um elemento de F_π. Agora, se w é um factor de $u_0 x_1^{+\infty}$ ou de $x_k^{-\infty} u_k$, então como por hipótese $u_0 x_1^{+\infty} = v_0 y_1^{+\infty}$ e $x_k^{-\infty} u_k = y_l^{-\infty} v_l$, é imediato que $w \in F_\rho$. Caso contrário, w é um factor de uma palavra biinfinita t da forma $t = x_i^{-\infty} u_i x_{i+1}^{+\infty}$, para algum $1 \leq i \leq k-1$. Então, $t \in I_\pi$ e como por hipótese $I_\pi = I_\rho$, tem-se que t também pertence a I_ρ. Mas se $t \in I_\rho$, então t é da forma:

- $t = y_j^{-\infty} v_j y_{j+1}^{+\infty}$ para algum $j \in \{1, \ldots, l-1\}$

ou da forma

- $t = y_j^\infty$ para algum $j \in \{1, \ldots, l\}$.

Na primeira situação, é imediato concluir que $w \in F_\rho$ (pois w é factor de $t = y_j^{-\infty} v_j y_{j+1}^{+\infty}$). Agora, se t é do segundo tipo, separemos o estudo em dois casos.

- Se $t = y_l^\infty$, então, como w é factor de t, w é também factor de $y_l^{-\infty}v_l$, tendo-se assim $w \in F_\rho$.

- Se $t = y_j^\infty$ para algum $j \in \{1, \ldots, l-1\}$, então w é factor de $y_j^{-\infty}v_j y_{j+1}^{+\infty}$, concluindo-se também neste caso que $w \in F_\rho$.

Mostramos assim que $F_\pi \subseteq F_\rho$. Por simetria, deduz-se a igualdade $F_\pi = F_\rho$, o que nos permite concluir que $\pi = \rho$.

Finalmente, provemos a decidibilidade da igualdade $\pi = \rho$. Como vimos anteriormente, isso equivale a mostrar que as igualdades $u_0 x_1^{+\infty} = v_0 y_1^{+\infty}$, $x_k^{-\infty}u_k = y_l^{-\infty}v_l$ e $I_\pi = I_\rho$ são decidíveis. É de notar que nestas igualdades entram apenas palavras $w \in A^{\mathbb{N}} \cup A^{-\mathbb{N}} \cup A^{\widetilde{\mathbb{Z}}}$ ultimamente periódicas que, portanto, admitem uma forma canónica (ver secções 2.2 e 2.3). Mais, essa forma canónica é efectivamente calculável uma vez que existem $t \in A^*$ e $u, v \in A^+$ tais que as referidas palavras w são já dadas sob a forma

- $w = tu^{+\infty}$ se w é uma palavra infinita à direita ;

- $w = u^{-\infty}t$ se w é uma palavra infinita à esquerda ;

- $w = u^\infty$ ou $w = u^{-\infty}tv^{+\infty}$ se w é uma palavra biinfinita.

Estamos assim, como pretendíamos, em condições de concluir que a igualdade $\pi = \rho$ é efectivamente decidível. $\square$

Observação 5.8 *Note-se que o teorema 5.7 mostra que cada ω-palavra $\pi \in \Omega_A^\omega$***LSl** *é caracterizada pelo triplo*

$$(p_{\mathbf{K}}(\pi), I_\pi, p_{\mathbf{D}}(\pi))$$

onde I_π é o conjunto de palavras biinfinitas descritas no enunciado.

Exemplo 5.9 *Seja $\pi \in \Omega_{\{a,b,c\}}^\omega$***LSl** *a ω-palavra dada por*

$$\pi = baac(ab^3acab^3ac)^\omega ab^2(ba)^\omega b((ba)^\omega b)^\omega.$$

Pelo Lema 5.6, π pode escrever-se na forma

$$\pi = baac(ab^3acab^3ac)^\omega ab^2(ba)^\omega b(ba)^\omega b(ba)^\omega b.$$

Note-se que $baac(ab^3acab^3ac)^{+\infty} = ba(acab^3)^{+\infty}$ *e que* $(ba)^{-\infty}b = (ab)^{-\infty}$. *Portanto podemos escrever* π, *por exemplo, sucessivamente nas formas*

$$\begin{aligned}\pi &= baac(ab^3acab^3ac)^\omega ab^2(ba)^\omega b(ba)^\omega b(ba)^\omega b\\ &= ba(acab^3)^\omega acab^2b(ab)^\omega(ba)^\omega bb(ab)^\omega\\ &= ba(acab^3)^\omega acab^3(ab)^\omega(ba)^\omega b^2(ab)^\omega\\ &= ba(acab^3)^\omega(ab)^\omega(ba)^\omega b^2(ab)^\omega.\end{aligned}$$

Para finalizar, consideremos $A = \{a, b, c\}$ e verifiquemos se **LSl** satisfaz a igualdade $\pi = \rho$, para $\pi, \rho \in \Omega_A^\omega\mathbf{S}$ tais que:

$$\pi = ab(ab^\omega ac)^\omega ac^\omega bc(ab)^\omega$$

$$\rho = (aba(b^\omega ca)^\omega)^\omega c(ba)^\omega b.$$

Considerando π e ρ em $\overline{\Omega}_A\mathbf{LSl}$ podemos escrever

$$\pi = abab^\omega acab^\omega acac^\omega bc(ab)^\omega$$

e

$$\begin{aligned}\rho &= aba(b^\omega ca)^\omega aba(b^\omega ca)^\omega c(ba)^\omega b\\ &= abab^\omega cab^\omega caabab^\omega cab^\omega cacb(ab)^\omega.\end{aligned}$$

Usando as notações da Observação 5.8 tem-se que as projecções de π e de ρ sobre o semigrupo $\Omega_A^\omega\mathbf{LSl}$ são respectivamente,

- $p_{\mathbf{LSl}}(\pi) = (abab^{+\infty}, I_\pi, (ab)^{-\infty})$;
- $p_{\mathbf{LSl}}(\rho) = (abab^{+\infty}, I_\rho, (ab)^{-\infty})$,

onde I_π e I_ρ são os conjuntos de palavras biinfinitas descritos no Teorema 5.7. Então,

$$I_\pi = \{b^\infty, c^\infty, (ab)^\infty, b^{-\infty}acab^{+\infty}, b^{-\infty}acac^{+\infty}, c^{-\infty}bc(ab)^{+\infty}\}$$

$$I_\rho = \{b^\infty, (ab)^\infty, b^{-\infty}cab^{+\infty}, b^{-\infty}caabab^{+\infty}, b^{-\infty}cacb(ab)^{+\infty}\}.$$

É assim imediato que $p_{\mathbf{LSl}}(\pi) \neq p_{\mathbf{LSl}}(\rho)$, e portanto $\mathbf{LSl} \not\models \pi = \rho$, apesar de **LI** satisfazer a igualdade pois as restrições de π e ρ a **LI** coincidem.

Capítulo 6

As ω-palavras sobre J

Este capítulo é dedicado ao estudo das operações implícitas sobre **J**, a pseudovariedade dos semigrupos $\mathcal{J}$-triviais, tendo por finalidade a resolução do problema da ω-palavra sobre essa pseudovariedade. Para alcançar esse objectivo comecemos com o estudo das operações implícitas sobre **DS**.

6.1 Operações implícitas sobre DS

Consideremos seguidamente a pseudovariedade

$$\mathbf{DS} = [\![[(ab)^\omega (ba)^\omega (ab)^\omega]^\omega = (ab)^\omega]\!] \; .$$

Note-se que

$$\mathbf{Sl} \subseteq \mathbf{J} \subseteq \mathbf{DS}.$$

É então imediato que as pseudovariedades **J** e **DS** verificam a condição da Proposição 4.3.

Vejamos agora que esta pseudovariedade pode ser caracterizada em termos de propriedades das relações de Green dos seus membros.

Proposição 6.1 *Seja S um semigrupo finito. São equivalentes as condições seguintes:*

1. *$S \in \mathbf{DS}$;*

2. *as $\mathcal{D}$-classes regulares de S são subsemigrupos;*

3. *cada $\mathcal{H}$-classe regular de S é um grupo;*

4. *se $r, s \in S$ são tais que $r \leq_{\mathcal{J}} s$ e r é regular, então $rs \,\mathcal{J}\, sr \,\mathcal{J}\, r$;*

5. *para cada idempotente $e \in S$, o conjunto dos elementos de S que estão $\mathcal{J}$ acima de e, i.e. $\{s \in S |\ e \leq_{\mathcal{J}} s\}$, é um subsemigrupo de S.*

Demonstração: É apresentada apenas a demonstração da implicação de 1 para 4 para ilustrar o tipo de técnicas usadas.
Consideremos $S \in \mathbf{DS}$ e sejam $r, s \in S$ tais que $r \leq_{\mathcal{J}} s$ e r é regular. Pretendemos então mostrar que $rs \,\mathcal{J}\, sr \,\mathcal{J}\, r$.

Comecemos por mostrar a seguinte propriedade: se $a, b \in S$, então $(ab)^\omega \,\mathcal{J}\, a(ab)^\omega$. Tem-se

$$a(ab)^\omega = a(ab)^\omega 1$$

e portanto $a(ab)^\omega \in S^1(ab)^\omega S^1$. Da definição de **DS** decorre que

$$(ab)^\omega = (ab)^\omega (ba)^{\omega-1} b\, \underline{a(ab)^\omega} [(ab)^\omega (ba)^\omega (ab)^\omega]^{\omega-1}$$

ou seja, $(ab)^\omega \in S^1 a(ab)^\omega S^1$. Conclui-se portanto que $(ab)^\omega \,\mathcal{J}\, a(ab)^\omega$.

Como r é regular, r admite algum inverso a. Tem-se então

$$r = rar = (ra)^\omega r.$$

Como consequência imediata da definição de **DS** e do facto de ra e ar serem idempotentes resulta que

$$\begin{aligned} r &= (ra)^\omega r \\ &= [(ra)^\omega (ar)^\omega (ra)^\omega]^\omega r \\ &= (raarra)^\omega r \\ &= (raarra)^{\omega-1} raa\underline{r}^2 ar. \end{aligned}$$

Logo, $r \,\mathcal{J}\, r^2$, e portanto, $r \,\mathcal{H}\, r^2$. Então a $\mathcal{H}$-classe de r é um grupo e $r \,\mathcal{J}\, r^\omega$.

Como por hipótese $r \leq_{\mathcal{J}} s$, existem $c, d \in S$ tais que $r = csd$. Portanto, usando a propriedade acima verificada, deduz-se

$$r \,\mathcal{J}\, r^\omega = (csd)^\omega \,\mathcal{J}\, cs(csd)^\omega \leq_{\mathcal{J}} sr^\omega \leq_{\mathcal{J}} sr \leq_{\mathcal{J}} r,$$

pelo que $r \,\mathcal{J}\, sr$. Mostra-se de forma análoga que $r \,\mathcal{J}\, rs$. $\square$

Corolário 6.2 *Seja* **V** *uma subpseudovariedade de* **DS**. *Se* $\pi, \rho \in \overline{\Omega}_A\mathbf{V}$ *são tais que* $\pi \leq_{\mathcal{J}} \rho$ *e* π *é regular, então* $\pi\rho \mathcal{J} \rho\pi \mathcal{J} \pi$.

O resultado seguinte é de particular interesse para o estudo a que nos propomos, as operações implícitas sobre **J**. Caracteriza as $\mathcal{J}$-classes regulares de $\overline{\Omega}_A\mathbf{V}$, quando **V** é uma subpseudovariedade de **DS** que contém **Sl**.

Proposição 6.3 *Seja* **V** *uma subpseudovariedade de* **DS** *contendo* **Sl** *e sejam* π *e* ρ *elementos regulares de* $\overline{\Omega}_A\mathbf{V}$. *Então,*

$$\pi \leq_{\mathcal{J}} \rho \;\Leftrightarrow\; c(\rho) \subseteq c(\pi).$$

Além disso, **DS** *é a maior pseudovariedade com esta propriedade.*

Demonstração: Comecemos por supor que $\pi \leq_{\mathcal{J}} \rho$. Então $\pi = \rho_1\rho\rho_2$ para alguns $\rho_1, \rho_2 \in \overline{\Omega}_A\mathbf{V}$ e portanto $c(\pi) = c(\rho_1\rho\rho_2)$. Como **V** contém **Sl** e $\overline{\Omega}_A\mathbf{Sl}$ é o semi--reticulado $\mathcal{P}(A)$ das partes do conjunto A, munido da união, conclui-se da Proposição 4.3 que

$$c(\rho_1\rho\rho_2) = c(\rho_1) \cup c(\rho) \cup c(\rho_2)$$

e consequentemente, tem-se $c(\rho) \subseteq c(\pi)$.

Suponhamos agora que $c(\rho) \subseteq c(\pi)$. Como o conteúdo é uma função contínua e $\overline{\Omega}_A\mathbf{Sl}$ é discreto, existe uma sucessão $(u_k)_k$ em $\Omega_A\mathbf{V}$ convergente para ρ tal que $c(u_k) = c(\rho)$ para todo o k. Suponhamos que para cada $k \in \mathbb{N}$, $u_k = a_{k,1}a_{k,2}\cdots a_{k,i_k}$. Como $c(u_k) = c(\rho)$, para todo o k, e $c(\rho) \subseteq c(\pi)$, então $a_{k,1} \in c(\pi)$. Portanto, pelo Lema 3.5, vem que $\pi \leq_{\mathcal{J}} a_{k,1}$ e, como por hipótese π é regular, o Corolário 6.2 permite deduzir que $\pi \mathcal{J} \pi a_{k,1}$. De modo análogo podemos mostrar que $\pi a_{k,1} \mathcal{J} \pi a_{k,1}a_{k,2}$ e, por recorrência, que

$$\pi \mathcal{J} \pi u_k.$$

Em particular, para cada $k \in \mathbb{N}$, existem $\beta_k, \delta_k \in \overline{\Omega}_A\mathbf{V}$ tais que $\pi = \beta_k u_k \delta_k$. Pela compacidade de $\overline{\Omega}_A\mathbf{V}$ podemos supor que as sucessões $(\beta_k)_k$ e $(\delta_k)_k$ são convergentes, digamos para β e δ, respectivamente. Assim, pela continuidade da multiplicação em $\overline{\Omega}_A\mathbf{V}$ tem-se $\pi = \beta\rho\delta$. Ou seja, $\pi \leq_{\mathcal{J}} \rho$.

Finalmente suponhamos que **W** é uma pseudovariedade que contém **Sl** tal que, se π e ρ são elementos regulares de $\overline{\Omega}_A\mathbf{W}$, então $\pi \leq_{\mathcal{J}} \rho$ se e só se $c(\rho) \subseteq$

$c(\pi)$. Sejam $\pi, \rho \in \overline{\Omega}_A\mathbf{W}$. Como **W** contém **Sl**, pela Proposição 4.3 vem que os elementos

$$((\pi\rho)^\omega(\rho\pi)^\omega(\pi\rho)^\omega)^\omega \text{ e } (\pi\rho)^\omega$$

têm o mesmo conteúdo. Uma vez que são elementos regulares, então, por hipótese, são $\mathcal{J}$-equivalentes. Tem-se ainda que $((\pi\rho)^\omega(\rho\pi)^\omega(\pi\rho)^\omega)^\omega \leq_{\mathcal{H}} (\pi\rho)^\omega$, e assim, da Proposição 1.23 (que é válida também para semigrupos compactos), resulta que $((\pi\rho)^\omega(\rho\pi)^\omega(\pi\rho)^\omega)^\omega$ e $(\pi\rho)^\omega$ estão na mesma $\mathcal{H}$-classe. Como os elementos são idempotentes, conclui-se do Corolário 1.22 que eles são iguais e portanto que $\mathbf{W} \subseteq \mathbf{DS}$. □

Como consequência desta última proposição temos o seguinte resultado.

Corolário 6.4 *Seja* **V** *uma subpseudovariedade de* **DS** *contendo* **Sl** *e sejam* π *e* ρ *elementos de* $\overline{\Omega}_A\mathbf{V}$. *Se* π *é regular e* $c(\rho) \subseteq c(\pi)$, *então* $\pi\rho$ *(resp.* $\rho\pi$*) é regular e* $\pi \,\mathcal{R}\, \pi\rho$ *(resp.* $\pi \,\mathcal{L}\, \rho\pi$*).*

Demonstração: Os elementos π e $(\pi\rho)^\omega$ têm o mesmo conteúdo (por hipótese $c(\rho) \subseteq c(\pi)$ e **V** contém **Sl**) e são regulares. Portanto, pela Proposição 6.3, $\pi \,\mathcal{J}\, (\pi\rho)^\omega$. Dado que $(\pi\rho)^\omega \leq_{\mathcal{J}} \pi\rho \leq_{\mathcal{J}} \pi$, deduzimos que $\pi\rho \,\mathcal{J}\, \pi$ e, em particular, que $\pi\rho$ é regular. Como $\pi\rho \leq_{\mathcal{R}} \pi$ tem-se, pela Proposição 1.23 (que é válida também para semigrupos compactos), que $\pi\rho \mathcal{R} \pi$. □

Introduzimos agora algumas noções necessárias para o que segue.

Sejam $w, u \in A^+$. Sendo $u = a_{i_1} \cdots a_{i_k}$, dizemos que u é uma *sub-palavra* de w se existe uma factorização de w da forma $w = w_0 a_{i_1} w_1 \cdots a_{i_k} w_k$ com $w_0, \ldots, w_k \in A^*$. Denotaremos por $\begin{bmatrix} w \\ u \end{bmatrix}$ o máximo dos inteiros r tais que u^r é uma sub-palavra de w. Por exemplo, $\begin{bmatrix} baccac \\ c \end{bmatrix} = 3$, $\begin{bmatrix} bacbabc \\ bc \end{bmatrix} = 2$ e $\begin{bmatrix} bacbabc \\ cb \end{bmatrix} = 1$.

Sejam $u \in A^+$ e **V** uma pseudovariedade que contém **J**. Então, a definição anterior pode ser generalizada a todos os elementos $\pi \in \overline{\Omega}_A\mathbf{V}$.

Proposição 6.5 (Almeida [4]) *Seja* **V** *uma pseudovariedade contendo* **J**. *Para cada alfabeto* A *e cada* $u \in A^+$, *a função*

$$\begin{array}{ccc} A^+ & \to & \mathbb{N}_0 \\ w & \mapsto & \begin{bmatrix} w \\ u \end{bmatrix} \end{array}$$

é uniformemente contínua para a topologia induzida pela distância d (definida na subsecção 3.2.2) e portanto prolonga-se de forma única a uma função contínua

$$\begin{array}{rcl} \overline{\Omega}_A\mathbf{V} & \rightarrow & \mathbb{N}_0 \cup \{\infty\} \\ \pi & \mapsto & \begin{bmatrix} \pi \\ u \end{bmatrix} \end{array}$$

onde $\mathbb{N}_0 \cup \{\infty\}$ *está munido da topologia do compactificado com um ponto do espaço discreto* $\mathbb{N}_0$.

Enquanto que o conteúdo serve para separar as $\mathcal{J}$-classes regulares dos semigrupos $\overline{\Omega}_A\mathbf{V}$, com $\mathbf{V}$ no intervalo $[\mathbf{J}, \mathbf{DS}]$, os parâmetros $\begin{bmatrix} - \\ u \end{bmatrix}$ podem ser utilizados para identificar os elementos regulares.

Lema 6.6 (Almeida [4]) *Sejam* $S \in \mathbf{DS}$ *e* $w \in A^+$, *com* $c(w) = \{a_{i_1}, \ldots, a_{i_k}\}$ *e seja* $u = a_{i_1} \cdots a_{i_k}$. *Se* $\begin{bmatrix} w \\ u \end{bmatrix} > |S|$, *então* $S \models w^{\omega+1} = w$.

O resultado seguinte dá-nos a caracterização dos elementos regulares de $\overline{\Omega}_A\mathbf{DS}$.

Teorema 6.7 (Almeida [4]) *Seja* $\mathbf{V}$ *uma pseudovariedade no intervalo* $[\mathbf{J}, \mathbf{DS}]$ *e seja* $\pi \in \overline{\Omega}_A\mathbf{V}$. *Então* π *é regular se e só se* $\begin{bmatrix} \pi \\ u \end{bmatrix} \in \{0, \infty\}$, *para todo o* $u \in A^+$.

Para finalizar, apresentamos um resultado que nos garante que cada operação implícita sobre **DS** é um produto finito de operações explícitas e de operações implícitas regulares. Este resultado é muito útil para o estudo que se segue.

Teorema 6.8 *Seja A um alfabeto. Toda a operação implícita* $\pi \in \overline{\Omega}_A\mathbf{S}$ *admite uma factorização da forma*

$$\pi = u_0\pi_1u_1 \cdots \pi_ku_k$$

onde

- $u_i \in A^*$ *para todo o* $i \in \{0, \ldots, k\}$, *e* $u_0 \neq 1$ *se* $\pi = u_0$;
- *a restrição a* **DS** *de cada* $\pi_1, \ldots, \pi_k \in \overline{\Omega}_A\mathbf{S}$ *é regular;*
- *se* $u_i = 1$, *com* $i \in \{1, \ldots, k-1\}$, *então* $c(\pi_i)$ *e* $c(\pi_{i+1})$ *são* $\subseteq$*-incomparáveis;*
- *para todo o* $i \in \{1, \ldots, k\}$, *tal que* $u_i \neq 1$ *(resp.* $u_{i-1} \neq 1$*), a primeira (resp. última) letra de* u_i *(resp.* u_{i-1}*) não pertence ao conteúdo de* π_i. □

6.2 Operações implícitas sobre J

Passemos ao estudo da pseudovariedade

$$\mathbf{J} = [\![(ab)^\omega a = (ab)^\omega = b(ab)^\omega]\!] = [\![(ab)^\omega = (ba)^\omega, a^\omega = a^{\omega+1}]\!] \,.$$

Nesta secção vamos mostrar que feitas as devidas simplificações na factorização descrita no Teorema 6.8, obtemos uma forma canónica para as operações implícitas sobre **J**.

Note-se que $\mathbf{N} \subseteq \mathbf{J}$ e portanto $\Omega_A\mathbf{J} = A^+$. Por outro lado, como $\overline{\Omega}_A\mathbf{J}$ é um semigrupo $\mathcal{J}$-trivial, os seus elementos regulares são idempotentes e, pela Proposição 6.3, são completamente determinados pelo seu conteúdo. Consequentemente, as operações implícitas regulares sobre **J** são da forma u^ω onde u é uma palavra sem letras repetidas. Portanto, pelo Teorema 6.8, podemos construir todos os elementos de $\overline{\Omega}_A\mathbf{J}$ a partir das projecções $a_1, \ldots, a_n$, utilizando um número finito de vezes duas operações: a multiplicação e a operação a^ω. Resulta então que todos os elementos de $\overline{\Omega}_A\mathbf{J}$ são ω-palavras, ou seja, $\overline{\Omega}_A\mathbf{J}$ coincide com $\Omega_A^\omega\mathbf{J}$.

Proposição 6.9 (Almeida[4]) *O ω-semigrupo $\overline{\Omega}_A\mathbf{J}$ é livre sobre A, na ω-variedade gerada por* **J**.

De seguida mostraremos como resolver o problema da palavra, que neste caso coincide com o problema da ω-palavra, para $\overline{\Omega}_A\mathbf{J}$. Ou seja, mostraremos como determinar de forma efectiva quando é que dois ω-termos nos geradores $a_1, \ldots, a_n$ são o mesmo elemento em $\overline{\Omega}_A\mathbf{J}$.

Para atacar este problema comecemos por tratar um outro. Como identificar a ω-variedade gerada por **J**?

Consideremos primeiro a ω-variedade $\mathcal{V}$ definida pelo conjunto Σ das identidades seguintes:

1) $(ab)c = a(bc)$;

2) $(ab)^\omega = (ba)^\omega = (a^\omega b^\omega)^\omega$;

3) $a^\omega a = a^\omega = a a^\omega$;

4) $(a^\omega)^\omega = a^\omega$.

Lema 6.10 *As identidades seguintes são consequências de* Σ*:*

i) $a^\omega a^\omega = a^\omega$;

ii) $(ab)^\omega a = (ab)^\omega = b(ab)^\omega$;

iii) $t^\omega = v^\omega$ *onde* t *é um termo e* v *é o produto, em qualquer ordem, das letras que ocorrem em* t.

Demonstração: No que segue , usaremos a notação $t =_n u$ para dizer que a igualdade dos ω-termos t e u é consequência das identidades n) de Σ.

i) Tem-se $a^\omega a^\omega =_4 (a^\omega)^\omega a^\omega =_3 (a^\omega)^\omega =_4 a^\omega$.

ii) A partir de Σ, podemos provar $(ab)^\omega = (ab)^\omega a$ da seguinte forma,

$$(ab)^\omega =_2 (b^\omega a^\omega)^\omega =_3 (b^\omega a^\omega)^\omega b^\omega a^\omega =_3 (b^\omega a^\omega)^\omega b^\omega a^\omega a =_3 (b^\omega a^\omega)^\omega a =_2 (ab)^\omega a.$$

De modo análogo, partindo de Σ podemos deduzir $b(ab)^\omega = (ab)^\omega$.

iii) Como $(a_1 \cdots a_r)^\omega =_{2,4} (a_1^\omega \cdots a_r^\omega)^\omega$, resta mostrar que, para qualquer permutação δ de $\{1, \ldots, r\}$, $\Sigma \vdash (a_1 \cdots a_r)^\omega = (a_{\delta_1}^\omega \cdots a_{\delta_r}^\omega)^\omega$ onde $\delta_i = \delta(i)$. De facto, partindo de Σ pode deduzir-se:

$$\begin{aligned}(a_1 \cdots a_r)^\omega &= [(a_{1+\delta_r} \cdots a_r a_1 \cdots a_{\delta_r})^\omega]^\omega, \text{ usando 4) e } (ab)^\omega = (ba)^\omega \\ &= [(a_1 \cdots a_r)^\omega a_{\delta_r}]^\omega, \text{ usando ii).}\end{aligned}$$

Repetindo sucessivamente o argumento anterior, obtém-se

$$\begin{aligned}(a_1 \cdots a_r)^\omega &= [(a_1 \cdots a_r)^\omega a_{\delta_1} \cdots a_{\delta_r}]^\omega, \\ &= [(a_1 \cdots a_r)^\omega (a_{\delta_1} \cdots a_{\delta_r})^\omega]^\omega, \text{ usando 4) e } (ab)^\omega = (a^\omega b^\omega)^\omega \\ &= (a_{\delta_1} \cdots a_{\delta_r})^\omega.\end{aligned}$$

O último passo verifica-se por aplicação de um processo análogo ao utilizado acima. □

Tendo em consideração as identidades de Σ e as suas consequências (Lema 6.10), podemos então proceder à redução de qualquer termo em $\{a_1, \ldots, a_n\}$ aplicando as seguintes regras:

rr.1) eliminar parenteses no que respeita à aplicação da operação binária de multiplicação;

rr.2) substituir por v^ω qualquer subtermo da forma t^ω, onde v é o produto, por ordem estritamente crescente dos índices, das variáveis que ocorrem em t;

rr.3) absorver em factores da forma v^ω quaisquer factores adjacentes nos quais ocorrem apenas variáveis de v.

Estas regras designam-se *regras de redução* e de facto reduzem efectivamente o comprimento dos termos. Assim, só se podem aplicar a um dado termo um número finito de vezes.

Repare-se ainda que a aplicação de uma das regras não colide nem impede a aplicação de uma das outras. Temos então um *sistema de regras de redução noetheriano* (ou de terminação finita) e *confluente* (i.e., se de um termo t, por aplicação das regras de redução, obtemos dois termos distintos t_1 e t_2, então, aplicando as regras de redução necessárias a t_1 e t_2 chegamos em ambos os casos a um termo comum t_3).

Na situação concreta que estamos a estudar, dado que $\{rr.1), rr.2), rr.3)\}$ é um conjunto de regras de redução noetheriano e confluente, então a partir de um qualquer ω-termo t sobre $\mathcal{V}$, obtém-se um e um só termo minimal t' (t' é minimal no sentido de não ser possível, por aplicação das regras de redução referidas, obter um outro termo de $\mathcal{V}$ distinto de t'). Diz-se então que t' é a forma canónica de t.

Passemos então a descrever as formas canónicas em estudo. Um ω-termo é chamado *explícito* ou uma *palavra* se nele não ocorre a operação unária. Se ele é da forma t^ω para algum termo t, então diz-se um *idempotente*. O conteúdo $c(t)$ de um dado termo t é o conjunto das variáveis que nele ocorrem. Portanto as formas canónicas são os termos da forma

$$t = t_1 t_2 \dots t_k,$$

onde

fc.1) cada t_i é uma palavra ou um idempotente;

fc.2) cada termo idempotente t_i é da forma v^ω, onde v é um produto de variáveis com os índices em ordem estritamente crescente;

fc.3) para dois termos idempotentes consecutivos t_i e t_{i+1}, os conjuntos $c(t_i)$ e $c(t_{i+1})$ são $\subseteq$-incomparáveis;

fc.4) dois termos consecutivos t_i e t_{i+1} não são ambos palavras;

fc.5) se t_i é uma palavra e t_{i+1} é um idempotente então a última letra de t_i não aparece em $c(t_{i+1})$;

fc.6) se t_{i+1} é uma palavra e t_i é um idempotente então a primeira letra de t_{i+1} não aparece em $c(t_i)$.

Se as formas canónicas de dois termos r_1 e r_2 coincidem, escrevemos $r_1 \simeq r_2$.

Note-se que a variedade $\mathcal{V}$ contém $\mathbf{J}$, pois todos os semigrupos $\mathcal{J}$-triviais satisfazem as identidades de Σ. Designando por $F_A\mathcal{V}$ o ω-semigrupo $\mathcal{V}$-livre sobre $A = \{a_1, \ldots, a_n\}$ temos portanto um homomorfismo sobrejectivo de ω-semigrupos

$$\varphi : \ F_A\mathcal{V} \ \rightarrow \ \overline{\Omega}_A\mathbf{J}$$

tal que $a_i \mapsto a_i$ com $i = 1, \ldots, n$.

Consideremos a relação $\equiv$ sobre $\overline{\Omega}_A\mathbf{J}$ definida por $\pi \equiv \rho$ se π e ρ têm as mesmas sub-palavras u de $\Omega_A\mathbf{S}$.

No que se segue o principal objectivo é mostrar que para dois termos t_1 e t_2,

$$t_1 \simeq t_2 \Leftrightarrow \varphi(t_1) \equiv \varphi(t_2). \tag{6.1}$$

Uma vez que Σ deduz a igualdade entre qualquer termo e a sua forma canónica, a implicação no sentido da esquerda para a direita é imediata. De facto,

$$t_1 \simeq t_2 \Rightarrow t_1 = t_2 \text{ em } F_A\mathcal{V} \Rightarrow \varphi(t_1) = \varphi(t_2) \Rightarrow \varphi(t_1) \equiv \varphi(t_2).$$

Da equivalência (6.1) e tendo em consideração a sequência de implicações apresentada, deduz-se que φ é uma bijecção (de facto φ é sobrejectiva e $\varphi(t_1) = \varphi(t_2) \Rightarrow \varphi(t_1) \equiv \varphi(t_2) \Leftrightarrow t_1 \simeq t_2 \Rightarrow t_1 = t_2$ em $F_A\mathcal{V}$), que $\simeq$ induz a igualdade em $F_A\mathcal{V}$ e ainda que $\equiv$ é a relação de igualdade em $\overline{\Omega}_A\mathbf{J}$.

Na equivalência (6.1), a prova da implicação no sentido da direita para a esquerda consiste em distinguir formas canónicas diferentes pela extracção de sub--palavras das suas imagens por φ. Comecemos por isolar o problema combinatório subjacente, definindo uma operação correspondente à extracção de sub-palavras directamente ao nível dos termos.

Para o que se segue consideremos um termo t fixado, em forma canónica, com a factorização $t = t_1 \cdots t_r$ satisfazendo as condições $(fc.1-6)$. Dizemos que uma palavra u pode ser extraída do termo t se existe uma factorização $u = u_1 \cdots u_r$ tal que

1. se t_i é explícito, então u_i é uma sub-palavra de t_i;
2. se t_i é idempotente, então $c(u_i) \subseteq c(t_i)$.

Uma tal factorização de u diz-se um modo de extrair u de t.

Consideremos um inteiro $k \geq 1$, e designemos por $t^{(k)}$ o termo obtido de t substituindo cada factor v^ω por v^k.

Lema 6.11 *Para uma palavra u são equivalentes as condições seguintes:*

1. *u é uma sub-palavra de $\varphi(t)$;*
2. *u é uma sub-palavra de $t^{(k)}$ para algum k;*
3. *u pode ser extraída de t.*

Note-se que os termos são expressões finitas nas variáveis e nas operações, e portanto não existe grande liberdade para proceder à extracção de palavras. Neste contexto o resultado seguinte é de grande interesse. A notação $\|t\|$ é utilizada para representar o número de factores idempotentes de t mais a soma dos comprimentos dos factores explícitos de t.

Lema 6.12 *Seja $k > \|t\|$. Então, para extrair de t uma palavra tendo um factor da forma w^k, com $|w| > 0$, tem-se necessariamente que um dos factores w daquela potência é extraído de algum factor idempotente e portanto, todos eles podem ser extraídos desse mesmo factor idempotente.*

Demonstração: Consideremos o refinamento da factorização canónica de t separando os factores explícitos em letras. Então o número total de factores de t é $\|t\|$ o qual, por hipótese, é inferior a k. Portanto em qualquer forma de extrair de t uma palavra tendo um factor da forma w^k com $|w| > 0$, algum dos w em

w^k tem de ser extraído completamente de um daqueles factores, o qual é então obrigatoriamente um idempotente. □

O resultado que se segue, tal como pretendido, estabelece a equivalência (6.1).

Teorema 6.13 *Dois ω-termos têm a mesma forma canónica se e só se as operações sobre* **J** *por eles induzidas têm as mesmas sub-palavras.*

Do estudo anterior resultam as seguintes conclusões importantes.

Teorema 6.14 *Para todo o alfabeto A, $\overline{\Omega}_A\mathbf{J}$ é o semigrupo livre com uma operação unária a^ω sobre A na variedade definida pelas identidades $(ab)^\omega = (ba)^\omega = (a^\omega b^\omega)^\omega$ e $a^\omega a = a^\omega = aa^\omega = (a^\omega)^\omega$. Dois termos nas variáveis $a_1, \ldots, a_n$ coincidem em $\overline{\Omega}_A\mathbf{J}$ se e só se eles têm a mesma forma canónica em relação às regras de redução $(rr.1-3)$. Em particular o problema da palavra para $\overline{\Omega}_A\mathbf{J}$ é decidível.*

Uma vez que o homomorfismo φ é uma bijecção, podemos falar da forma canónica de uma operação implícita sobre **J**. Podemos obter uma definição directa deste conceito substituindo a palavra "termo" por "operação" na definição de forma canónica de termos. Recordemos que um elemento idempotente de $\overline{\Omega}_A\mathbf{J}$ é completamente caracterizado pelo seu conteúdo. Assim, um idempotente de $\overline{\Omega}_A\mathbf{J}$ pode ser denotado por (B) onde B é o seu conteúdo.

Teorema 6.15 *Seja A um alfabeto. Toda a operação implícita $\pi \in \overline{\Omega}_A\mathbf{J}$ admite uma factorização da forma*

$$\pi = u_0(B_1)u_1 \cdots (B_k)u_k$$

onde

- *$u_i \in A^*$ para todo $0 \leq i \leq k$, e $u_0 \neq 1$ se $\pi = u_0$;*
- *se $u_i = 1$, com $1 \leq i \leq k-1$, então B_i e B_{i+1} são $\subseteq$-incomparáveis;*
- *para todo $1 \leq i \leq k$, tal que $u_{i-1} \neq 1$, a última letra de u_{i-1} não aparece em B_i;*
- *para todo $1 \leq i \leq k$, tal que $u_i \neq 1$ a primeira letra de u_i não aparece em B_i.*

Uma factorização de π deste tipo é dita em forma canónica.

Teorema 6.16 *Sejam $\pi = u_0(B_1)u_1 \cdots (B_k)u_k$ e $\rho = v_0(C_1)v_1 \cdots (C_m)v_m$ duas factorizações em forma canónica de elementos de $\overline{\Omega}_A\mathbf{J}$. Então são equivalentes as condições seguintes:*

1. *$\pi = \rho$;*

2. *π e ρ têm as mesmas sub-palavras;*

3. *$k = m$, $u_0 = v_0$, $u_i = v_i$ e $B_i = C_i$ $(i = 1, \ldots, k)$.*

Para terminar este capítulo, apresentemos um exemplo concreto.

Exemplo 6.17 *Consideremos o alfabeto $A = \{a, b, c, d\}$ e as operações implícitas π, ρ e β de $\Omega_A^\omega\mathbf{S}$ tais que:*

- $\pi = cab(ab^\omega a)^\omega ac^\omega bc(ab)^\omega a$;

- $\rho = (ab(a^\omega b)^\omega cab^{\omega+1}c)^\omega abc^\omega dc(ac)^\omega ba$;

- $\beta = ((a^\omega b)^\omega cab^\omega)^\omega acda(ac^\omega ac)^\omega cba$.

Por aplicação das regras de redução, anteriormente referidas, deduz-se que as formas canónicas das projecção de π, ρ e β sobre o semigrupo $\Omega_A^\omega\mathbf{J}$ são dadas, respectivamente, por:

- $p_\mathbf{J}(\pi) = c(\{a, b\})(\{c\})bc(\{a, b\})$;

- $p_\mathbf{J}(\rho) = (\{a, b, c\})d(\{a, c\})ba$;

- $p_\mathbf{J}(\beta) = (\{a, b, c\})d(\{a, c\})ba$.

Conclui-se portanto que $\mathbf{J} \not\models \pi = \rho$, pois $p_\mathbf{J}(\pi)$ e $p_\mathbf{J}(\rho)$ admitem formas canónicas distintas. Contrariamente, $\mathbf{J} \models \rho = \beta$ pois as formas canónicas de $p_\mathbf{J}(\rho)$ e de $p_\mathbf{J}(\beta)$ coincidem.

Em suma, o problema da palavra para o semigrupo livre $\overline{\Omega}_A\mathbf{J}$ é resolvido descrevendo regras de transformação de operações que permitem reduzir a "complexidade" das operações até obter "formas canónicas" para as operações. A igualdade de duas operações, no semigrupo livre em causa, é então testada construindo as suas formas canónicas pela aplicação das regras de redução e verificando se elas são iguais.

Capítulo 7

Desenvolvimentos

Uma pseudovariedade $\mathbf{V}$ diz-se *decidível* se existe um algoritmo que, dado um semigrupo S qualquer, permita decidir se S pertence a $\mathbf{V}$.

Em teoria de semigrupos há um operador que generaliza o produto directo e desempenha um papel de grande importância: trata-se do chamado *produto semidirecto*. O produto semidirecto $\mathbf{V} * \mathbf{W}$ de duas pseudovariedades $\mathbf{V}$ e $\mathbf{W}$ é a classe dos divisores de produtos semidirectos $S * T$ com $S \in \mathbf{V}$ e $T \in \mathbf{W}$.

Em meados da década de 60 Krohn e Rhodes [28] estabeleceram que todo o semigrupo finito pertence a algum produto semidirecto iterado da forma $\mathbf{A} * (\mathbf{G} * \mathbf{A})^n$, com $n \in \mathbb{N}$, onde $\mathbf{G}$ é a pseudovariedade de todos os grupos finitos e $\mathbf{A}$ é a pseudovariedade de todos os semigrupos finitos aperiódicos. Tal deu origem à noção de *complexidade* de um semigrupo finito S que é precisamente o menor n tal que $S \in \mathbf{A} * (\mathbf{G} * \mathbf{A})^n$. O problema de determinar a complexidade de um semigrupo é desde então um dos principais problemas da teoria de semigrupos finitos, e está portanto relacionado com a decidibilidade de produtos semidirectos iterados envolvendo as pseudovariedades dos grupos e dos semigrupos aperiódicos.

A decidibilidade de pseudovariedades não é preservada por alguns dos mais comuns operadores de pseudovariedades [1, 30]. Em particular, Rhodes [30] mostrou que existem pseudovariedades decidíveis cujo produto semidirecto não é decidível. Deste facto surgiu a necessidade de estabelecer condições mais fortes que a decidibilidade, na expectativa de que fossem decidíveis as pseudovariedades obtidas pela aplicação de operadores a pseudovariedades com tais propriedades. Neste contexto, Almeida e Steinberg [9] introduziram a noção de *mansidão*. A mansidão consiste num refinamento do conceito de *hiperdecibilidade* anteriormente introduzido por Almeida [5].

Como referimos no início do capítulo 4, uma *assinatura implícita* é um conjunto σ de operações implícitas contendo a multiplicação $a \cdot b$. A *assinatura canónica* $\kappa = \{a \cdot b, a^\omega\}$ é normalmente a mais usada na teoria de semigrupos finitos quando se trabalha com pseudovariedades aperiódicas. Para um alfabeto A e uma pseudovariedade $\mathbf{V}$, denotamos por $\Omega_A^\sigma \mathbf{V}$ o σ-subsemigrupo de $\overline{\Omega}_A \mathbf{V}$ gerado por A. Os elementos de $\Omega_A^\sigma \mathbf{V}$ dizem-se *σ-palavras* sobre $\mathbf{V}$.

Uma pseudovariedade $\mathbf{V}$ diz-se *σ-mansa* se: $\mathbf{V}$ é recursivamente enumerável, $\mathbf{V}$ é σ-redutível e o problema da σ-palavra é decidível para $\mathbf{V}$. Se uma pseudovariedade $\mathbf{V}$ é σ-mansa para alguma assinatura σ, tal que σ é recursivamente enumerável e é constituída por operações implícitas computáveis, então $\mathbf{V}$ diz-se *mansa*. Note-se que a assinatura canónica referida satisfaz estas condições.

A mansidão implica a decidibilidade. No entanto a questão de saber se a mansidão é útil para provar a decidibilidade de pseudovariedades obtidas pela aplicação dos operadores de pseudovariedades mais comuns é ainda um problema em aberto. De facto, em [9], Almeida e Steinberg pensaram ter conseguido provar que o produto semidirecto iterado de pseudovariedades *mansas* seria decidível. Dado que a pseudovariedade $\mathbf{G}$ dos grupos é mansa [16], a validade de tal resultado teria como corolário que a função *complexidade* de Krohn-Rhodes poderia ser efectivamente calculada, ficando apenas dependente da prova de que a pseudovariedade $\mathbf{A}$ é mansa (resultado anunciado por Rhodes mas ainda não publicado). Infelizmente a prova de que o produto semidirecto iterado de pseudovariedades *mansas* seria decidível baseava-se num resultado de 1995 cuja validade foi posta em causa e ainda não foi demonstrada.

Em geral, provar a mansidão de uma pseudovariedade não é fácil. Conhecem-se já bastantes pseudovariedades que se sabe serem mansas. No entanto, muitas outras bem conhecidas continuam a ocupar os investigadores. Sabe-se por exemplo que:

- **Ab** é mansa [10];
- **K** e **D** são mansas [12];
- $\mathbf{LSl} = \mathbf{Sl} * \mathbf{D}$ é mansa [22];
- **R** é mansa [11].

Foi precisamente a questão da mansidão da pseudovariedade **R**, para a assinatura canónica $\kappa = \{a \cdot b, a^\omega\}$, que motivou o recente trabalho de J. Almeida e M. Zeitoun [13, 14], onde se encontra resolvido, em particular, o problema da ω-palavra sobre a pseudovariedade **R**. Apresenta-se de seguida um breve resumo da resolução desse problema. Para mais detalhe consultar [13, 14].

Contrariamente ao que se poderia esperar, o problema da ω-palavra para a pseudovariedade **R** não foi resolvido descrevendo um conjunto confluente finito de regras de redução, que aplicadas repetidamente até que nenhuma redução mais seja possível conduzisse a uma forma canónica de uma ω-palavra, de tal forma que duas ω-palavras sobre **R** são iguais se e só se têm a mesma forma canónica. Uma vez não encontrado tal sistema foi conjecturada a sua inexistência.

Nesse trabalho é usada uma nova representação das operações implícitas sobre **R**, as chamadas *árvores binárias*. Tais árvores são regulares, isto é, elas podem ser dobradas em certos autómatos finitos pela identificação de subárvores isomorfas, se e somente se as operações implícitas que representam são ω-palavras. Para além disso, tais autómatos são usados para descrever um algoritmo que resolve o problema da ω-palavra sobre a pseudovariedade **R**.

Para $\pi \in \overline{\Omega}_A\mathbf{S}$, uma factorização da forma

$$\pi = \pi_1 a \pi_2$$

em que $a \in A$, $\pi_1, \pi_2 \in \overline{\Omega}_A\mathbf{S}$, $a \notin c(\pi_1)$ e $c(\pi_1 a) = c(\pi)$ é dita uma *factorização básica à esquerda* de π.

Exemplo 7.1 *Consideremos o alfabeto* $A = \{a, b, c\}$ *e as* ω*-palavras* π, ρ *de* $\Omega_A^\omega \mathbf{S}$ *tais que*

$$\pi = (ab^\omega c)^\omega$$

e

$$\rho = a^\omega bc(ab^\omega c)^\omega.$$

A factorização básica à esquerda de cada uma das ω*-palavras referidas é dada, respectivamente por*

$$\pi = \pi_1 \cdot c \cdot \pi_2$$

e

$$\rho = \rho_1 \cdot c \cdot \rho_2,$$

em que $\pi_1 = ab^\omega$, $\pi_2 = (ab^\omega c)^{\omega-1}$, $\rho_1 = a^\omega b$ *e* $\rho_2 = (ab^\omega c)^\omega$.

Teorema 7.2 *Sejam* $\pi, \rho \in \overline{\Omega}_A \mathbf{S}$ *e suponhamos que* $\pi = \pi_1 a \pi_2$ *e* $\rho = \rho_1 b \rho_2$ *são factorizações básicas à esquerda. Então* $\mathbf{R}$ *satisfaz* $\pi = \rho$ *se e só se* $a = b$ *e* $\mathbf{R}$ *satisfaz* $\pi_1 = \rho_1$ *e* $\pi_2 = \rho_2$.

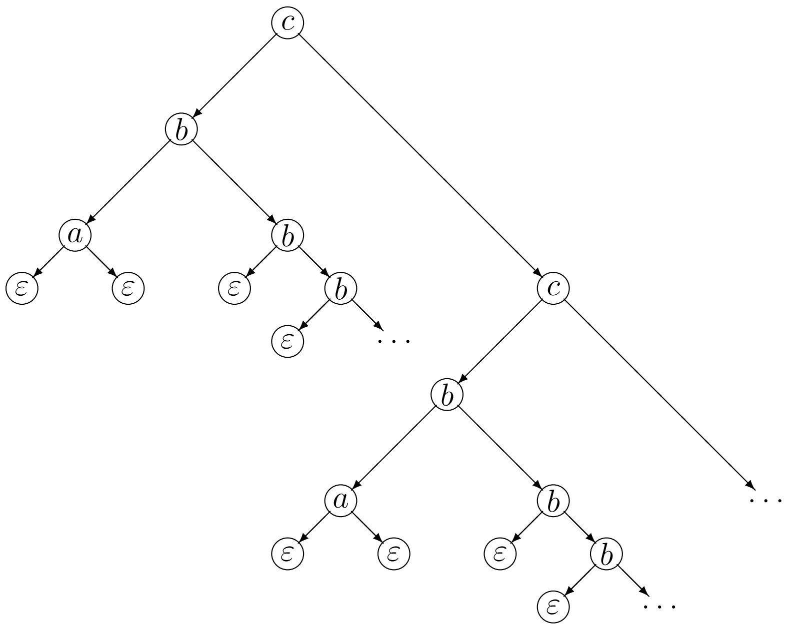
A árvore binária, de vértices etiquetados em $A \cup \{\varepsilon\}$, construída, como descrevemos de seguida, por iteração da factorização básica à esquerda de uma operação implícita π denota-se por $\mathcal{T}(\pi)$ e é chamada a $\mathbf{R}$-árvore de π. Seja $\pi = \pi_1 a \pi_2$ a factorização básica à esquerda de π. Então a raíz de $\mathcal{T}(\pi)$ tem etiqueta a e as subárvores à esquerda e à direita são obtidas pela iteração desta construção sobre π_1 e π_2, respectivamente. Por exemplo, retomando $\pi = (ab^\omega c)^\omega$ do Exemplo 7.1, a factorização básica à esquerda de π_1 é

$$\pi_1 = a \cdot b \cdot b^{\omega-1}$$

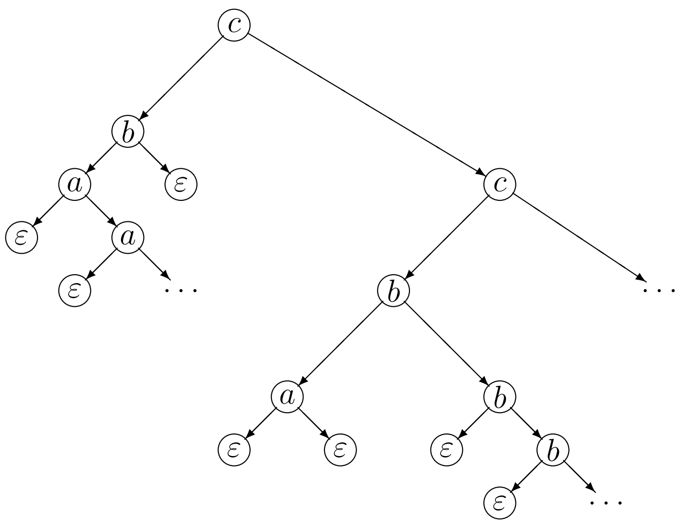
e a de π_2 é

$$\pi_2 = ab^\omega \cdot c \cdot (ab^\omega c)^{\omega-2}.$$

Iterando este processo obtém-se a árvore infinita descrita na figura seguinte, onde ε representa a palavra vazia.



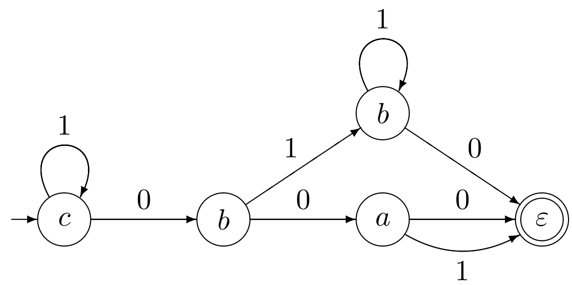
Agora para $\rho = a^\omega bc(ab^\omega c)^\omega$ do Exemplo 7.1, tem-se que a factorização básica à esquerda de ρ_1 é $\rho_1 = a^\omega \cdot b \cdot \varepsilon$ e a de ρ_2 é $\rho_2 = ab^\omega \cdot c \cdot (ab^\omega c)^{\omega-1}$. Iterando este processo obtém-se a árvore infinita descrita na figura seguinte.

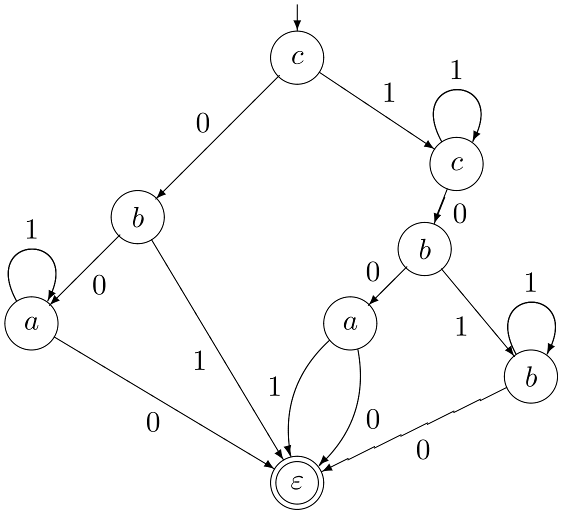


Note-se que na última árvore apresentada a parte que se repete sucessivamente é apenas o segundo ramo.

Do Teorema 7.2 pode deduzir-se a caracterização da igualdade das operações implícitas sobre **R** nos termos da igualdade das suas **R**-árvores. Assim, tendo em consideração o exposto, podemos concluir que **R** não satisfaz a igualdade entre as ω-palavras π e ρ do Exemplo 7.1 pois como se pode observar as suas **R**-árvores são distintas. Note-se que a pseudovariedade **R** contém **K**, portanto, tendo em consideração o estudo realizado na subsecção 4.1.3, conclui-se imediatamente que **R** não satisfaz a igualdade entre as ω-palavras π e ρ, uma vez que estas são distintas sobre **K**. Refira-se ainda que apesar de distintas sobre **K** e sobre **R**, sobre **J** as ω-palavras referidas são iguais.

Como já foi mencionado, dada uma operação implícita π sobre **R** se π é representada por alguma ω-palavra então a sua **R**-árvore pode ser dobrada num **R**-autómato associado a π que é finito. Este **R**-autómato é chamado o **R**-autómato minimal de π e é representado por $\mathcal{A}(\pi)$. Assim, dado que as operações implícitas π e ρ do Exemplo 7.1 são ω-palavras, as suas **R**-árvores, apresentadas anteriormente, podem ser dobradas nos **R**-autómatos minimais seguintes, associados a π e ρ respectivamente.





Usa-se a transição etiquetada com 0 para indicar deslocamento para a esquerda e com 1 para a direita, a seta entrante, mais pequena, representa o estado inicial que corresponde à raíz e o círculo duplo representa o estado final que corresponde às folhas da árvore.

Note-se que $\mathcal{A}(\pi)$ é o autómato quociente de $\mathcal{T}(\pi)$ com a congruência $\sim_\pi$, na qual dois nós são equivalentes se as subárvores dos seus descendentes são idênticas.

Corolário 7.3 *As seguintes condições são equivalentes para um par de operações implícitas π e ρ:*

1. $\mathbf{R} \models \pi = \rho$;
2. $\mathcal{T}(\pi) = \mathcal{T}(\rho)$;
3. $\mathcal{A}(\pi) = \mathcal{A}(\rho)$.

No trabalho referido [13, 14] descrevem-se algoritmos que permitem dada uma ω-palavra π determinar $\mathcal{A}(\pi)$ em tempo linear. Tendo em conta o Corolário 7.3, isto dá-nos a solução para o problema da ω-palavra sobre $\mathbf{R}$

Teorema 7.4 (Almeida e Zeitoun [14]) *O problema da ω-palavra sobre $\mathbf{R}$ é decidível.*

Bibliografia

[1] D. Albert, R. Baldinger e J. Rhodes, Undecidability of the identity problem for finite semigroups, J. Symbolic Logic 57 (1992), 179-192.

[2] J. Almeida. Some pseudovariety joins involving the pseudovariety of finite groups, *Semigroup Forum* **37**(1988) 53-57.

[3] J. Almeida. The algebra of implicit operations, *Algebra Universalis* **26** (1989) 16-72.

[4] J. Almeida. *Finite semigroups and Universal Algebra*, World Scientific, Singapore, 1994.

[5] J. Almeida. Hyperdecidable pseudovarieties and the calculation of semidirect products, *Int. J. Algebra Comput.* **9** (1999) 241-261.

[6] J. Almeida e A. Azevedo. Implicit operations on certain classes of semigroups, em S. Goberstein e P. Higgins (Eds.), Proc. of Chico Conf., *Semigroups and their applications*, D. Reidel (1987) 1-11.

[7] J. Almeida e A. Azevedo. The join of the pseudovarieties of $\mathcal{J}$-trivial e $\mathcal{L}$--trivial semigroups, *J. Pure and Applied Algebra* **60** (1989) 129-137.

[8] J. Almeida, A. Azevedo e M. Zeitoun. Pseudovariety joins involving $\mathcal{J}$-trivial and completely regular semigroups, *Int. J. Algebra and computation* **9** (1999) 99-112.

[9] J. Almeida e B. Steinberg. On the decidability of iterated semidirect products and applications to complexity, Proc. London Math Soc. **80** (2000) 50-74.

[10] J. Almeida e M. Delgado. Tameness of the pseudovariety of abelian groups, Int. J. Algebra and Computation, **15** (2005) 327-338.

[11] J. Almeida, J. C. Costa e M. Zeitoun. Tameness of pseudovariety joins involving **R**, Monatshefte für Mathematik, **146** (2005) 89-111.

[12] J. Almeida e M. Zeitoun. Tameness of some locally trivial pseudovarieties, Communications in Algebra **31** (2003) 61-77.

[13] J. Almeida e M. Zeitoun. An automatha-theoretical approach to the word problem for ω-terms over **R**, Tech. Report CMUP 2004-38, Univ. Porto, 2004, submetido.

[14] J. Almeida e M. Zeitoun. The equational theory of ω-terms for finite $\mathcal{R}$-trivial semigroups. Proceedings of the Workshop on Semigroups and Languages, World Scientific, Singapore (2004) 1-22.

[15] J. Almeida e P Weil. Relatively free profinite monoids : an introduction and examples, em J. Fountain (Ed.), *Semigroups, formal languages and groups*, Kluwer (1995) 73-117.

[16] C. Ash. Inevitable graphs: A proof of the type II conjecture and some related decision procedures, *Int. J. Algebra and Comput.* **1** (1991) 127-146.

[17] A. Azevedo. *Operações implícitas sobre pseudovariedades de semigrupos. Aplicações.* Tese de Doutoramento, Universidade do Porto, 1989.

[18] A. Azevedo. The join of the pseudovarieties **J** with permutative pseudovarieties, em Almeida e al.(Eds.), *Lattices, Semigroups and Universal Algebra*, Plenum, New York (1990) 1-11.

[19] J. C. Costa. *Autómatos e máquinas de Turing*, publicação do Departamento de Matemática da Universidade do Minho, 2004.

[20] J. C. Costa. Pseudovariedades da forma $\mathbf{V}^{-1}\mathbf{W}$. Trabalho de síntese apresentado às "Provas de Aptidão Pedagógica e Capacidade Científica", Universidade do Minho, 1993.

[21] J. C. Costa. Quelques intersections de variétés de semigroupes finis et de variétés de langages, opérations implicites. Tese de Doutoramento, Universidade de Paris **6**, 1998.

[22] J. C. Costa e M. L. Teixeira. Tameness of the pseudovariety **LSl**, Int. J. Algebra and Computation **14** (2004) 627-654.

[23] J. C. Costa. Tópicos de Álgebra, Manuscrito, Universidade do Minho, 2004.

[24] S. Eilenberg. *Automata, Languages and Machines*, Vol. B, Academic Press, New York, 1976.

[25] P. A. Grillet. Semigroups: An Introduction to the Structure Theory, Marcel Dekker, New York, 1995.

[26] J. Howie. *Fundamentals of Semigroups Theory*, Oxford University Press, New York, 1995.

[27] J.-E. Pin. Variétés de langages formels, Masson, Paris, 1984.

[28] K. Krohn e J. Rhodes. *Algebraic theory of machines I - Prime decomposition theorem for finite semigroups and machines*, Trans. Amer. Math. Soc. **116** (1965) 450-464.

[29] J. Reiterman. The Birkhoff theorem for finite algebras, *Algebra Universalis* **14** (1982) 1-10.

[30] J. Rhodes. Undecidability, automata and pseudovarieties of finite semigroups, *Int. J. Algebra Comput.* **9** (1999) 455-473.

[31] Lothaire. *Combinatorics on words*, Addison-Welsey Publishing Company,1983.

[32] M. Morse e G. A. Hedlund. Symbolic dynamics, Amer. J. Math. **60** (1938) 815-866.

[33] P. Vieira. Palavras finitas e infinitas. Dissertação de Mestrado, Universidade de Lisboa, 2003.

Índice